Jason "Jay" Barnes (*pro hac vice*)
jaybarnes@simmonsfirm.com
Eric Johnson (*pro hac vice*)
ejohnson@simmonsfirm.com
An Truong (*pro hac vice*)
atruong@simmonsfirm.com
Sona R. Shah (*pro hac vice*)
sshah@simmonsfirm.com
SIMMONS HANLY CONROY LLP
112 Madison Avenue, 7th Floor
New York, NY 10016
Telephone: 212.784.6400
Facsimile: 212.213.5949

Christian Levis (*pro hac vice*)
clevis@lowey.com
Amanda Fiorilla (*pro hac vice*)
afiorilla@lowey.com
Rachel Kesten (*pro hac vice*)
rkesten@lowey.com
Yuanchen Lu (*pro hac vice*)
ylu@lowey.com
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: 914.997.0500
Facsimile: 914.997.0035

Michael W. Sobol (SBN 194857)
msobol@lchb.com
David T. Rudolph (SBN 233457)
drudolph@lchb.com
Linnea D. Pittman (*pro hac vice*)
lpittman@lchb.com
Danna Elmasry (*pro hac vice*)
delmasry@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111
Telephone: 415.956.1000
Facsimile: 415.956.1008

Philip L. Fraietta (SBN 354768)
pfraietta@bursor.com
Max S. Roberts (*pro hac vice forthcoming*)
mroberts@bursor.com
Victoria X. Zhou (*pro hac vice forthcoming*)
vzhou@bursor.com
Joshua R. Wilner (SBN 353949)
jwilner@bursor.com
BURSOR & FISHER, P.A.
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: 646.837.7150
Facsimile: 212.989.9163

Attorneys for Plaintiffs and the Proposed Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE THE TRADE DESK, INC. DATA PRIVACY LITIGATION

Case No. 3:25-cv-2889 (CRB)

CONSOLIDATED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

Page

I. INTRODUCTION

1. The Trade Desk, Inc. (hereafter "Trade Desk" or "Defendant") engages in the mass collection, use, and sale of highly-detailed personal information about tens of millions of people in the United States. Trade Desk operates one of the world's largest "demand-side" platforms, through which it bids on ad space on the Internet on behalf of advertisers. In the course of operating its business, Trade Desk incessantly surveils Americans' conduct both online and in real space. Trade Desk collects Americans' Internet browsing habits across their internet-connected devices and their real-world movements and activities, and combines it with vast troves of data about their health, politics, religion, sexuality, finances, and life habits. It then makes the data in these massive dossiers available for sale through various products and services to third parties, who can subsequently use that data to further surveil and manipulate people.

2. Trade Desk creates detailed dossiers on Americans by (1) tagging them with a permanent identification number; (2) collecting their activity and communications on the Internet and across their phones, computers, and connected TVs; (3) collecting information about their offline activities, such as their geolocation and real-world purchases; and (4) bringing all this information together in a single profile maintained by Trade Desk. Trade Desk then facilitates the sale of information in these dossiers through products and services—including those offered within the "Real Time Bidding" ecosystem—an online advertising auction system that uses people's sensitive personal information to target them for digital advertising across their phones, computers, and connected TVs. Through the Trade Desk, third parties use these vast amounts of sensitive data tied to specific individuals for internet advertising and other forms of manipulation.

3. Trade Desk has accomplished this even though (and perhaps because) virtually no consumer has ever heard of it, no consumer has ever actually consented to any of its activities in question here, and no consumer has a meaningful ability to opt-out of its tracking, dossier building, or dossier sales unless they forego use of the Internet altogether.

4. Plaintiffs bring this action on behalf of themselves and others similarly situated to enforce their fundamental Constitutional, common law, and statutory rights to privacy, which Trade Desk has violated and continues to violate, and to seek permanent injunctive relief in the form of

an order ensuring their ability to participate in modern society without Trade Desk surveilling their activities and creating profiles about them without their consent.

II. PLAINTIFFS

A. Plaintiff Doug Michie

5. Plaintiff Doug Michie resides in Ventura, California. Like most members of modern society, Plaintiff Michie must use the Internet to conduct routine affairs of daily life.

6. On January 31, 2025, Plaintiff Michie received a data access request response that consisted of a Microsoft Excel file[1] from Trade Desk, indicating that the company had tracked, compiled, and analyzed his personal information, including geolocation, web browsing activities, and real-world activities, thereby creating a comprehensive profile of him. Trade Desk used this information to place him into thousands of data "segments," (described below) and to sell access to information about him to the highest advertising bidder through nearly instantaneous Real-Time Bidding ("RTB") auctions. On information and belief, Trade Desk continues to track Plaintiff Michie's internet activity, enrich the profile it maintains of him, and make access to his personal information available to third parties without his consent.

7. The data access request file consists of two Excel sheets, one labeled "BidFeedback Results" and one labeled "DMP Results."

1. "BidFeedback" Results Excel File

8. Upon information and belief, Trade Desk's "BidFeedback Results" Excel sheet represents information about Plaintiff Michie that Trade Desk collected and/or sold through RTB auctions between November 4, 2024 and January 31, 2025 (the latter being the date on which Plaintiff Michie received this file). On information and belief, the file demonstrates both that Trade Desk tracked, compiled, and analyzed Plaintiff Michie's web browsing, geolocation, and other personal information, and that it used it to facilitate advertising targeting him.

9. The "BidFeedback Results" Excel sheet demonstrates that Trade Desk tracked Plaintiff Michie's activity on hundreds of websites, including the interception and collection of his

[1] In order to protect Plaintiff Michie's privacy, the data access request Excel file is not attached to this Complaint.

searches for and views of content related to politics, mental health, and personal finance. Trade Desk's tracking mechanisms, as described below at paragraphs 88–107, were present on a variety of those websites, including at the time that Plaintiff Michie accessed them. Those tracking mechanisms transmitted to Trade Desk his URL data, coupled with unique identifiers that Trade Desk used to associate his browsing history with other data compiled into a data profile of him.

10. The "BidFeedback Results" Excel sheet demonstrates that Trade Desk assigned to Plaintiff Michie an inescapable and persistent "Unified ID 2.0" ("UID2")—the equivalent of a universal "online social security number" used to track, profile, and persistently surveil him, as described in detail below. Trade Desk used the UID2 mechanism to connect Plaintiff Michie's online activities into a single identity profile through its "identity graph," as described below.

11. The "BidFeedback Results" Excel file further shows that Trade Desk used this identity profile to enable the sale of instantaneous ad placement via RTB "bid requests." The data associated with these bid requests, as reflected in the file, include at least the following personal information associated with Plaintiff Michie:

a. **Trade Desk IDs or "TDIDs":** The spreadsheet contains a column with several "TDIDs" associated with Plaintiff Michie's single UID2. TDIDs are a type of "persistent" cookie identifier that Trade Desk stored on Plaintiff Michie's browser even after he closed out of a browsing session or switched devices, allowing Trade Desk to track and identify Plaintiff Michie across the Internet.[2]

b. **Mapped UID2 to other IDs:** The file shows how Trade Desk connected Plaintiff Michie's UID2 to other identifiers, including his device advertising IDs.

c. **IP addresses:** Trade Desk connected several IP addresses to Plaintiff Michie's UID2.

d. **Metro area and city:** Trade Desk identified the area code and city associated with Plaintiff Michie's internet activities and devices.

[2] *The Trade Desk Glossary*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/resources/doc/Glossary [https://perma.cc/76BF-9YBF].

e. **Device type, make, model, and browser:** Trade Desk tracked Plaintiff Michie across his devices, collecting and storing information about them, to deliver ads everywhere he might see them, including his phone, computer, and connected Roku TV.

f. **Precise latitude and longitude:** The sheet contains the precise latitude and longitude that Trade Desk associated with each bid, *i.e.*, the precise latitude and longitude where Plaintiff Michie was viewing the particular websites where the ads were placed.[3]

g. **Websites viewed:** The "BidFeedback Results" Excel sheet shows that Trade Desk tracked Plaintiff Michie's activity on at least hundreds of websites. The top-level domains[4] of websites visited by Plaintiff Michie and where Trade Desk tracked Plaintiff's communications and interactions with those websites, as reflected in the "BidFeedback Results" Excel sheet, include but are not limited to:

h. www.cbsnews.com

i. www.sfgate.com

j. www.investopedia.com

k. www.verywellmind.com

2. <u>"DMP Results" Excel File</u>

12. On information and belief, the "DMP Results" Excel file demonstrates that through its "Demand-Side Platform" ("DSP") and its "data marketplace"—described in more detail below—Trade Desk also facilitated the sale of access to hundreds of thousands of "segments" associated with Plaintiff Michie. Trade Desk partners with data suppliers to make Plaintiff Michie's personal information and information derived or inferred from his data available to third party advertisers. A "segment," according to Trade Desk, is "a group of users that can be targeted as an audience because they share a defining characteristic, such as gender, region, or an action that

[3] *REDS Impressions Feed Columns*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/reds/doc/Impressions?r=imc-aas&ref=adtechexplained.com [https://perma.cc/5FS2-E84E].

[4] In order to protect Plaintiffs' privacy, the specific pages they viewed within these domains are not included in the Complaint. However, as alleged herein, the specific pages are information that Trade Desk intercepted and collected through its invasive and surreptitious technology.

they've taken online."[5] This innocuous description obscures that Trade Desk actually maintains tens of thousands of such "segments" associated with each individual, based on highly sensitive information such as their race, religion, political views, health conditions, financial patterns, and sexual activities, as described below. The number of data segments targeting Plaintiff Michie over a relatively short period is staggering—the DMP Results Excel file contains more than 32,000 unique segments, which touch on every aspect of Plaintiff Michie's life. For example, among the 32,340 unique segments Trade Desk associated with Plaintiff Michie are segments relating to:

a. **Politics:** In addition to containing segments about Plaintiff Michie's voting history and patterns, and even his propensity to watch certain political TV programs, the file contains segments for sale indicating his views on a range of sensitive political issues including abortion, gun control, environmental regulation, the kind of car he drives, immigration and border control, defunding the police, U.S. support of Ukraine, and the war in Israel. These segments allow advertisers, including political campaigns, as discussed below, to target and manipulate Plaintiff Michie with incredible precision on issues they not only know he cares about, but for which they know exactly where he stands.

b. **Physical and mental health:** Also for sale are segments about Plaintiff Michie's physical and mental health, including his past and present health insurance, the physical conditions from which he suffers, when and what types of medicine he takes, and his shopping patterns for specific brands of foods, beverages, and healthcare products. Trade Desk has even amassed segments about his personality and emotional states.

c. **Financial health and patterns:** Trade Desk offers advertisers segments about Plaintiff Michie's income; mortgages, including the monthly payment amount; banking habits, including the number and types of credit cards he has; credit score and history of timely paying credit card balances; spending patterns across numerous categories of expenses; approach to investing and personal finance; and other aspects of his financial health, including information related to paying off student loans.

---

[5] *The Trade Desk Glossary*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/resources/doc/Glossary [https://perma.cc/76BF-9YBF].

d. **Personal shopping preferences and habits:** Among the segments is a staggering level of detail about what Plaintiff Michie purchases from which grocery stores, and how often. The grocery store segments alone paint a detailed tableaux of his food and alcohol preferences. The segments also indicate Plaintiff Michie's tendency to research purchases before making them, where he likes to travel, and what he likes to do on vacation. They indicate what Plaintiff Michie watches, reads, and listens to, and broadly capture how he spends his time.

3. Trade Desk's Further Interception and Use of Plaintiff Michie's Online Browsing Activity

13. In addition to the information contained in the files sent to Plaintiff Michie by Trade Desk, on information and belief, Trade Desk continues to track Plaintiff Michie's online and offline activity, enrich its profile of him, and make his personal information available to third parties without his consent. Plaintiff Michie has visited websites where his electronic communications were intercepted by the use of Trade Desk code, as described below.

14. The full scope and extent of Trade Desk's tracking and compiling of Plaintiff Michie's online and offline activity and personal information resides with Trade Desk itself, is not fully disclosed by Trade Desk, and therefore must be determined through discovery from Trade Desk. Based on a reasonable investigation, Plaintiff Michie alleges as follows.

15. Trade Desk has tracked Plaintiff Michie's activity on at least thousands of websites, intercepting and collecting his searches and viewing of content related to health, sexual, and personal financial issues on numerous websites. Trade Desk's tracking mechanisms—including "cookies," "pixels," and JavaScript code—as described below at paragraphs 88–107, were present on those websites.

16. Those tracking mechanisms transmitted the websites' URL data to Trade Desk, along with unique identifiers that Trade Desk used to associate browsing history with other data compiled into a dossier about Plaintiff Michie. Trade Desk's wiretapping and pen register code—which transmits to Trade Desk domains including but not limited to "insight.adsrvr.org" and "direct.adsrvr.org"—was present on websites visited by Plaintiff, which, in turn, transmitted to Trade Desk the content of Plaintiff Michie's communications and interactions with the websites, including the precise content read, products viewed, and searches queried, as well as routing,

addressing, or signaling information related to these online interactions. Trade Desk maintains a data profile about Plaintiff Michie and provides access to that profile, via products or services derived from the profile, to unknown third parties. Trade Desk has engaged in this conduct throughout the class period.

17. The top-level domains[6] of websites visited by Plaintiff Michie where Trade Desk's tracking mechanisms have been detected include but are not limited to:

a. Menshealth.com

b. Ehealthinsurance.com

c. Medicalnewstoday.com

d. Verywellhealth.com

e. Healthcare.gov

f. Foxnews.com

g. Theguardian.com

h. Economist.com

i. Newsweek.com

j. Usbank.com

k. Ameriprise.com

l. Vanguard.com

m. Wsfsbank.com

n. Findlaw.com

B. Plaintiff Justin Dyer

18. Plaintiff Justin Dyer resides in Sunnyvale, California. Like most members of modern society, he must use the Internet to conduct routine affairs of daily life.

19. On January 31, 2025, Plaintiff Dyer received a data access request Excel file[7] from Trade Desk, generated from the data Trade Desk associates with Plaintiff Dyer's email address.

[6] In order to protect Plaintiffs' privacy, the specific pages they viewed within these domains are not included in the Complaint.

[7] Out of respect for Plaintiff Dyer's privacy, the data access request Excel file is not attached to this Complaint.

The Excel file indicates that Trade Desk had tracked, compiled, and analyzed his personal information, including geolocation, web browsing activities, and offline activities, and thereby created a comprehensive profile of him. Trade Desk used that comprehensive profile to enable advertisers to place Plaintiff Dyer into sensitive data segments, and, upon information and belief, to sell information about him to the highest advertising bidder in nearly instantaneous real-time bidding ("RTB") auctions. On information and belief, Trade Desk continues to track Plaintiff Dyer's internet activity, enrich the profile it maintains of him as described below, and make his personal information available to third parties without his consent.

20. The data access request file consists of a single Excel sheet labeled "DMP Results." The sheet contains more than 39,000 rows of sensitive segment data targeting Plaintiff Dyer. Trade Desk sent the file with no explanatory materials.

21. Upon information and belief, Trade Desk also tracked, compiled, and analyzed Plaintiff Dyer's web browsing, geolocation, and other personal information, which Trade Desk used to enable advertisers to place him into sensitive data segments as discussed below.

22. Upon information and belief, Trade Desk assigned to Plaintiff Dyer an inescapable and persistent UID2 used to track, profile, and persistently surveil him, as described in detail below. Trade Desk used the UID2 mechanism to connect Plaintiff Dyer's online activities into a single identity profile through its identity graph, as described below, which contained detailed demographic information about him, as well as his email addresses.

1. "DMP Results" Excel File

23. Through both its "Demand-Side Platform" ("DSP") and its "data marketplace", Trade Desk facilitated the sale of thousands of "segments" associated with Plaintiff Dyer. The number of data segments targeting Plaintiff Dyer is staggering—the DMP Results Excel file contains more than 15,000 unique segments, which touch on every aspect of Plaintiff Dyer's life.

24. For example, among the 15,235 unique segments Trade Desk has associated with Plaintiff Dyer are segments about:

a. **Politics:** In addition to segments about Plaintiff Dyer's voting history, his household's political affiliation by party, and donations to certain causes, the file contains segments

for sale indicating his views on a range of sensitive political issues including: the environment and climate change, increasing the minimum wage, immigration reform and border security, LGBTQ support, *Roe v. Wade*, the Second Amendment, holding companies accountable for bad behavior, marijuana legalization, and tax reform. These segments allow advertisers, including political campaigns, as discussed below, to target and manipulate Plaintiff Dyer with incredible precision on issues they not only know he cares about, but for which they know exactly where he stands.

b. **Physical health and health purchasing habits:** Also for sale are segments about Plaintiff Dyer's physical health and his purchasing habits related to physical conditions and his health and wellbeing. They include segments about the physical conditions from which he suffers, including a recent accident injury, his *propensity* to develop certain health conditions in the future, why he takes medicine and what brand(s) he purchases, and his shopping patterns for specific foods, beverages, and healthcare products, including based on location such as proximity to his home.

c. **Financial health and patterns:** Trade Desk's data marketplace offers advertisers segments about Plaintiff Dyer's income; banking habits, including his comfort level with trusting money to banking institutions; credit score and history of making timely card payments; spending patterns and habits; and other aspects of his financial wellbeing.

d. **Personal shopping preferences and habits:** Among the segments is a staggering level of detail about where Plaintiff Dyer purchases groceries (including based on proximity to his home), what he buys, and even what time of day he tends to shop. The grocery store segments alone paint a detailed tableaux of his food and alcohol preferences, and his activities related to those preferences. The segments also indicate when and where Plaintiff Dyer likes to travel. They indicate what activities and hobbies he engages in, and even information about his pets.

2. Trade Desk's Further Interception and Use of Plaintiff Dyer's Online Browsing Activity

25. In addition to the information contained in the file Trade Desk sent to Plaintiff Dyer, on information and belief, Trade Desk continues to track Plaintiff Dyer's online and offline activity,

enrich the profile of him as described below, and make his personal information available to third parties without his consent. Plaintiff Dyer has visited websites where his electronic communications were intercepted by the use of Trade Desk code, as described below.

26. The full scope and extent of Trade Desk's tracking and compiling of Plaintiff Dyer's online and offline activity and personal information resides with Trade Desk itself, is not fully disclosed by Trade Desk, and therefore must be determined through discovery from Trade Desk. Based on a reasonable investigation, Plaintiff Dyer alleges as follows.

27. Trade Desk has tracked Plaintiff Dyer's activity on at least thousands of websites, including intercepting and collecting Plaintiff Dyer's searches for and views of articles related to health and personal financial issues on numerous websites. Trade Desk's tracking mechanisms—including "cookies," "pixels," and JavaScript code—as described below at paragraphs 88–107, were present on those websites.

28. Those tracking mechanisms transmitted the websites' URL data to Trade Desk, along with unique identifiers that Trade Desk used to associate browsing history with other data, compiled into a data profile of Plaintiff Dyer. Trade Desk's wiretapping and pen register code—which transmits to Trade Desk domains including but not limited to "insight.adsrvr.org" and "direct.adsrvr.org"—was present on websites visited by Plaintiff Dyer. This code transmitted to Trade Desk the content of his communications and interactions with the websites, including the precise content read, products viewed, and searches queried, as well as routing, addressing, or signaling information related to these online interactions. Trade Desk maintains a data profile about Plaintiff Dyer and provides access to that profile, via products or services derived from the profile, to unknown third parties. Trade Desk engaged in this conduct throughout the class period.

29. Trade Desk tracked Plaintiff Dyer's specific activity on thousands of websites, including the interception and collection of Plaintiff's searches for and views of content related to his physical health and healthcare, personal finance and taxes, and firearms. Trade Desk's tracking mechanisms, as described below at paragraphs 63–82, were present on those websites, including at the time Plaintiff Dyer accessed them. Those tracking mechanisms transmitted to Trade Desk the

websites' URL data coupled with unique identifiers that Trade Desk used to associate that browsing history with other data compiled into a data profile of him.

30. The top-level domains of websites visited by Plaintiff Dyer where Trade Desk's tracking mechanisms have been detected include but are not limited to:

a. Healthcare.gov

b. Lendingclub.com

c. Cabelas.com

d. Apartments.com

e. Taxact.com

f. Credit.com

g. Mypremiercreditcard.com

h. Cigna.com

i. Everydayhealth.com

j. Healthnet.com

k. Credit.com

l. Foxnews.com

C. Plaintiff Jessica Ju

31. Plaintiff Jessica Ju resides in Monterey Park, California. Like most members of modern society, Plaintiff Ju must use the Internet to conduct routine affairs of daily life.

32. On June 27, 2025, Plaintiff Ju received a data access request response that consisted of a Microsoft Excel file[8] from Trade Desk, indicating that the company had tracked, compiled, and analyzed her personal information, including geolocation, web browsing activities, and real-world activities, and thereby created a comprehensive profile of her. Trade Desk used this information to place her into thousands of data "segments," (described below) and to sell access to information about her to the highest advertising bidder through nearly instantaneous Real-Time Bidding ("RTB") auctions. On information and belief, Trade Desk continues to track Plaintiff Ju's

[8] In order to protect Plaintiff Ju's privacy, the data access request Excel file is not attached to this Complaint.

internet activity, enrich the profile it maintains of her, and make access to her personal information available to third parties without his consent.

33. The data access request file consists of two Excel sheets, one labeled "BidFeedback Results" and one labeled "DMP Results."

1. "BidFeedback" Results Excel File

34. Upon information and belief, Trade Desk's "BidFeedback Results" Excel sheet represents information about Plaintiff Ju that Trade Desk collected and/or sold through RTB auctions between April 11, 2025 and June 27, 2025 (the latter being the date on which Plaintiff Ju received this file). On information and belief, the file demonstrates both that Trade Desk tracked, compiled, and analyzed Plaintiff Ju's web browsing, geolocation, and other personal information, and that it used it to facilitate advertising targeting her.

35. The "BidFeedback Results" Excel sheet demonstrates that Trade Desk tracked Plaintiff Ju's activity on numerous websites, via Trade Desk's tracking mechanisms as described below at paragraphs 88–107, which were present at the time that Plaintiff Ju accessed them. Those tracking mechanisms transmitted to Trade Desk her URL data, coupled with unique identifiers that Trade Desk used to associate her browsing history with other data compiled into a data profile of her.

36. The "BidFeedback Results" Excel sheet demonstrates that Trade Desk assigned to Plaintiff Ju an inescapable and persistent UID2 to track, profile, and persistently surveil her, as described in detail below. Trade Desk used the UID2 mechanism to connect Plaintiff Ju's online activities into a single identity profile through its "identity graph," as described below.

37. The "BidFeedback Results" Excel sheet further shows that Trade Desk used this identity profile to enable the sale of instantaneous ad placement via RTB "bid requests." The data associated with these bid requests, as reflected in the file, include at least the following personal information associated with Plaintiff Ju:

a. **Trade Desk IDs or "TDIDs":** The spreadsheet contains a column with several "TDIDs" associated with Plaintiff Ju's single UID2. TDIDs are a type of "persistent" cookie identifier that Trade Desk stored on Plaintiff Ju's browser even after she closed out of a browsing

session or switched devices, allowing Trade Desk to track and identify Plaintiff Ju across the Internet.[9]

b. **Mapped UID2 to other IDs:** The file shows how Trade Desk connected Plaintiff Ju's UID2 to other identifiers, including her device advertising IDs.

c. **IP addresses:** Trade Desk connected several IP addresses to Plaintiff Ju's UID2.

d. **Metro area and city:** Trade Desk identified the area code and city associated with Plaintiff Ju's internet activities and devices.

e. **Device type, make, model, and browser:** Trade Desk tracked Plaintiff Ju across her devices, collecting and storing information about them, to deliver ads everywhere she might see them, including her phone and computer.

f. **Precise latitude and longitude:** The sheet contains the precise latitude and longitude that Trade Desk associated with each bid, *i.e.*, the precise latitude and longitude where Plaintiff Ju was viewing the particular websites where the ads were placed.[10]

g. **Websites viewed:** The "BidFeedback Results" Excel sheet shows that Trade Desk tracked Plaintiff Ju's activity on numerous websites. The top-level domains of websites visited by Plaintiff Ju and where Trade Desk tracked Plaintiff's communications and interactions with those websites, as reflected in the "BidFeedback Results" Excel sheet, include but are not limited to:

a. Accuweather.com

b. Reuters.com

c. Apnews.com

2. <u>"DMP Results" Excel File</u>

38. On information and belief, the "DMP Results" Excel file demonstrates that through its "Demand-Side Platform" ("DSP") and its "data marketplace"—described in more detail

[9] *The Trade Desk Glossary*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/resources/doc/Glossary [https://perma.cc/76BF-9YBF].

[10] *REDS Impressions Feed Columns*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/reds/doc/Impressions?r=imc-aas&ref=adtechexplained.com [https://perma.cc/5FS2-E84E].

below—Trade Desk also facilitated the sale of access to tens of thousands of "segments" associated with Plaintiff Ju. Trade Desk partners with data suppliers to make Plaintiff Ju's personal information and information derived or inferred from her data available to third party advertisers. A "segment," according to Trade Desk, is "a group of users that can be targeted as an audience because they share a defining characteristic, such as gender, region, or an action that they've taken online."[11] This innocuous description obscures that Trade Desk actually maintains tens of thousands of such "segments" associated with each individual, based on highly sensitive information such as their race, religion, political views, health conditions, financial patterns, and sexual activities, as described below. The number of data segments targeting Plaintiff Ju over a relatively short period is staggering—the DMP Results Excel file contains more than 27,000 unique segments, which touch on every aspect of Plaintiff Ju's life. For example, among the 27,685 unique segments Trade Desk associated with Plaintiff Ju are segments relating to:

a. **Politics:** In addition to segments about Plaintiff Ju's voter demographic information, political party preference, and voting habits, the file contains segments for sale indicating her views on a range of sensitive political issues including her opinion on the attempted assassination of Donald Trump and the events of January 6.

b. **Physical and mental health:** Also for sale are segments about Plaintiff Ju's physical and mental health. These segments include information regarding specific health conditions, whether she is a known buyer of specific types of medication, and the types of physical exercises in which she engages.

c. **Financial health and patterns:** Trade Desk's data marketplace also offers advertisers segments about Plaintiff Ju's spending patterns across numerous categories of expenses, approach to investing and personal finance, and other aspects of her financial health. Examples of these segments include information about her mortgage, profile information about the type of investor she is, her annual insurance expenditures, and information about her credit cards.

[11] *The Trade Desk Glossary*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/resources/doc/Glossary [https://perma.cc/76BF-9YBF].

d. **Personal shopping preferences and habits:** Among the segments is a staggering level of detail about what Plaintiff Ju purchases from which grocery stores, and how often. Examples of these segments include: how often she spends money on travel, how involved her pre-purchase research is likely to be, whether she eats out frequently, whether she is interested in discount or high-end shopping, the specific media she consumes, what specific grocery items she purchases, and whether she considers herself an ethical consumer.

3. Trade Desk's Further Interception and Use of Plaintiff Ju's Online Browsing Activity

39. In addition to the information contained in the files sent to Plaintiff Ju by Trade Desk, on information and belief, Trade Desk continues to track Plaintiff Ju's online and offline activity, enrich its profile of her, and make her personal information available to third parties without her consent. Plaintiff Ju has visited websites where her electronic communications were intercepted by the use of Trade Desk code, as described below.

40. The full scope and extent of Trade Desk's tracking and compiling of Plaintiff Ju's online and offline activity and personal information resides with Trade Desk itself, is not fully disclosed by Trade Desk, and therefore must be determined through discovery from Trade Desk. Based on a reasonable investigation, Plaintiff Ju alleges as follows.

41. Trade Desk's invasive online tracking spans thousands of websites. Trade Desk eavesdropped, intercepted, and collected Plaintiff Ju's activity on numerous websites, including intercepting and collecting her searches and viewing of content related to health, sexual, and personal financial issues on numerous websites. Trade Desk's tracking mechanisms—including "cookies," "pixels," and JavaScript code—as described below at paragraphs 88–107, were present on those websites.

42. Those tracking mechanisms transmitted the websites' URL data to Trade Desk, along with unique identifiers that Trade Desk used to associate browsing history with other data compiled into a dossier about Plaintiff Ju. Trade Desk's wiretapping and pen register code—which transmits to Trade Desk domains including but not limited to "insight.adsrvr.org" and "direct.adsrvr.org"—was present on websites visited by Plaintiff Ju, which, in turn, transmitted to

Trade Desk the content of Plaintiff Ju's communications and interactions with the websites, including the precise content read, products viewed, and searches queried, as well as routing, addressing, or signaling information related to these online interactions. Trade Desk maintains a data profile about Plaintiff Ju and provides access to that profile, via products or services derived from the profile, to unknown third parties. Trade Desk has engaged in this conduct throughout the class period.

43. The top-level domains of websites visited by Plaintiff Ju where Trade Desk's tracking mechanisms have been detected include but are not limited to:

a. Aircanada.com

b. Chase.com

c. Chewy.com

d. Healthy.kaiserpermanente.org

e. Zillow.com

f. Hyatt.com

g. Southwest.com

D. Plaintiff Jennifer Turner

44. Plaintiff Jennifer Turner resides in Tulare, California. Like most members of modern society, she must use the Internet to conduct routine affairs of daily life.

45. On July 16, 2025, Plaintiff Turner submitted a data access request to Trade Desk as is her right under the California Consumer Privacy Act (CCPA) as a California resident. As of the date of this filing, Plaintiff has not received a response to her request.

46. Upon information and belief, Trade Desk tracked, compiled, and analyzed Plaintiff Turner's personal information, including geolocation, web browsing activities, and offline activities, and thereby created a comprehensive profile of her that is as expansive as those reflected in the data from Trade Desk received by Plaintiffs Michie, Dyer, and Ju. Upon information and belief, Trade Desk used that comprehensive profile to enable advertisers to place Plaintiff Turner into sensitive data segments, and to sell information about her to the highest advertising bidder in nearly instantaneous real-time bidding ("RTB") auctions. On information and belief, Trade Desk

continues to track Plaintiff Turner's internet activity, enrich the profile it maintains of her, and make her personal information available to third parties without her consent.

47. Upon information and belief, Trade Desk assigned to Plaintiff Turner an inescapable and persistent UID2 used to track, profile, and persistently surveil her, as described in detail below. Trade Desk used the UID2 mechanism to connect Plaintiff Turner's online activities into a single identity profile through its identity graph, as described below.

1. Trade Desk's Further Interception and Use of Plaintiff Turner's Online Browsing Activity

48. Upon information and belief, in addition to the information Trade Desk would compile in response to a data access request about Plaintiff Turner, Trade Desk continues to track Plaintiff Turner's online and offline activity, enrich the profile of her as described below, and make her personal information available to third parties without her consent. Plaintiff has visited websites where her electronic communications were intercepted by Trade Desk code, as described below.

49. The full scope and extent of Trade Desk's tracking and compiling of Plaintiff Turner's online and offline activity and personal information resides with Trade Desk itself, is not fully disclosed by Trade Desk, and therefore must be determined through discovery from Trade Desk. Based on a reasonable investigation, Plaintiff Turner alleges as follows.

50. Trade Desk's invasive online tracking spans across thousands of websites. Trade Desk eavesdropped, intercepted, and collected Plaintiff Turner's activity on numerous websites, including intercepting and collecting her searches and viewing of content relating to health, via Trade Desk's tracking mechanisms—including "cookies," "pixels," and JavaScript code—as described below at paragraphs 88–107.

51. Those tracking mechanisms transmitted the websites' URL data to Trade Desk, along with unique identifiers that Trade Desk used to associate browsing history with other data compiled into a dossier about Plaintiff Turner. Trade Desk's wiretapping and pen register code—which transmits to Trade Desk domains including but not limited to "insight.adsrvr.org" and "direct.adsrvr.org"—was present on websites visited by Plaintiff, which, in turn, transmitted to Trade Desk the content of Plaintiff Turner's communications and interactions with the websites,

including the precise content read, products viewed, and searches queried, as well as routing, addressing, or signaling information related to these online interactions. Trade Desk maintains a data profile about Plaintiff Turner and provides access to that profile, via products or services derived from the profile, to unknown third parties. Trade Desk has engaged in this conduct throughout the class period.

52. Trade Desk tracked Plaintiff Turner's specific activity across websites and other online services. Trade Desk's tracking mechanisms, as described below at paragraphs 88–107, were present on those websites, including at the time Plaintiff Turner accessed them. Those tracking mechanisms transmitted to Trade Desk the websites' URL data coupled with unique identifiers that Trade Desk used to associate that browsing history with other data compiled into a data profile of her.

53. The top-level domains of websites visited by Plaintiff Turner where Trade Desk's tracking mechanisms have been detected include but are not limited to:

a. Noom.com

b. Gohenry.com

c. Usatoday.com

d. Starz.com

e. Amtrak.com

f. Directv.com

g. Cvs.com

h. Riteaid.com

i. Etsy.com

III. DEFENDANT

54. Trade Desk is a Delaware Corporation headquartered at 42 North Chestnut Street, Ventura, California.

IV. JURISDICTION AND VENUE

55. This Court has personal jurisdiction over Defendant Trade Desk, because it is headquartered in California and the actions giving rise to this case took place in this District.

56. This Court has subject matter jurisdiction over the federal claims in this action pursuant to 28 U.S.C. § 1331.

57. This Court has subject matter jurisdiction over this entire action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because this is a class action in which the amount in controversy exceeds $5,000,000, excluding interests and costs.

58. This Court also has supplemental jurisdiction over the state law claims in this action pursuant to 28 U.S.C. § 1367, because the state law claims form part of the same case or controversy as those that give rise to the federal claims.

59. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) and (b)(2), because Plaintiff Justin Dyer resides within this District, because Trade Desk maintains substantial business operations in this District, and because a substantial part of the events or omissions giving rise to the claims described herein occurred in this District. Upon information and belief, activities enabling Trade Desk's identity resolution products, Unified ID 2.0, Data Management Platform including managing data partnerships, and facilitating the sale of data through RTB auctions, as discussed in this complaint, take place in this District.

V. CHOICE OF LAW

60. California law governs the substantive legal issues in this case. The State of California has a significant interest in regulating the conduct of businesses operating within its borders.

61. Trade Desk's principal place of business is California, where it maintains the "nerve center" of its business activities—the place where its high-level officers direct, control, and coordinate the corporation's activities, including its marketing, software development, and major policy, financial, and legal decisions.

62. Trade Desk's privacy-invasive conduct as described herein emanated from, and was conceived and executed in, California.

63. Under California's choice of law principles, which are applicable to this action, the common law of California applies to the common law claims of the Class members.

VI. DIVISIONAL ASSIGNMENT

64. Pursuant to Civil L.R. 3-2(c), assignment to this division is proper because a substantial part of the conduct which gives rise to Plaintiffs' claims occurred in this District. Trade Desk's conduct as described below is directed at Internet users and people throughout the United States, including in San Francisco County, California.

VII. FACTS COMMON TO ALL CLAIMS

A. Trade Desk's Practices are Inherently Privacy-Invasive.

65. Trade Desk has developed and implemented a series of interwoven systems and technologies that are designed to track individuals across the Internet, collect as much information about them as possible, and build massive but precise and detailed profiles about their interests, preferences, and behaviors. Trade Desk accomplishes this data mining and surveillance using tracking technologies seeded throughout the Internet (online) and augmented by third-party data partnerships (offline, *i.e.*, in the physical world).

66. Trade Desk has been described as a "giant[] in online advertising," on par with Google and Amazon.[12] But unlike Google and Amazon—which consumers have at least heard of and often have direct and contractual relationships with—internet users have no idea that Trade Desk is collecting, compiling, and analyzing their personal information through incessant and pervasive surveillance. This ignorance is by design. Trade Desk's practices as described herein are deliberately opaque and designed to take place in the shadows, without internet users' awareness—and therefore without their consent.

67. While Trade Desk is largely unknown to the populace it surveils, Trade Desk publicly articulates a vision of the world where there is no anonymity or privacy on the Internet. It argues that Internet users must agree to a "value exchange" by which they surrender their anonymity in order to access "free" content on the "open internet" (*i.e.*, the Internet outside of the "walled

---

[12] Answer and Defenses of Respondent Propel Media, Inc. at 3, *In re IQVIA Holdings, Inc.*, No. 9416, FEDERAL TRADE COMMISSION (July 31, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/608325_-_efile0002584_-answer_and_defenses_of_respondent_propel_media_inc._public_3.pdf [https://perma.cc/TCS8-L63P].

gardens" such as Meta, Google, and X) so that their personal information can be ceaselessly collected and monetized.[13] To that end, Trade Desk stalks users across the Internet and their devices relentlessly, impinging on their private activities without their knowledge or consent.

68. The breadth of information that Trade Desk tracks and collects is staggering. The subsequent precision of its Internet user profiling is alarming and highly offensive. With respect to profiling information, Trade Desk tracks and collects almost every facet of an individual's activity. From that information, Trade Desk is able to infer a wide and accurate range of behavioral traits, interests, and attributes related to gender, race, ethnicity, religion, health, drug use, and sex life or sexual orientation. Alongside its never-ending online surveillance of individual's online activity, Trade Desk tracks and collects a range of unique identifiers—including emails and phone numbers that it uses to anchor and assign UID2s—from which it can directly identify individual users across all of their various devices.

69. Among other things, Trade Desk leverages this vast amount of precise information to participate on behalf of its advertising clients in Real-Time Bidding ("RTB") auctions. RTB is an online advertising auction system that uses personal information, such as browsing history, location, demographics, and offline activity, to determine which digital ad will be displayed to a user on a given website or application.[14]

70. When a user loads a webpage or app, an RTB auction for ad space to be shown to that user takes place without the user's knowledge. Supply side platforms, which "enable[] publishers to manage and automate the selling of their ad inventory"[15] send user data, known as "bidstream data," to advertising exchanges. Those advertising exchanges then broadcast this data

---

[13] *'A value exchange': How consumers can benefit from a new era of authentication*, THE CURRENT (Jan. 8, 2024), https://www.thecurrent.com/value-exchange-consumers-can-benefit-era-authentication-identity [https://perma.cc/CDB4-KYA6].

[14] *See*, *e.g.*, Sara Georghegan, *What is Real Time Bidding?,* ELECTRONIC PRIVACY INFORMATION CENTER (Jan. 15, 2025), https://epic.org/what-is-real-time-bidding [https://perma.cc/K93B-AF6Z]; *What is Real Time Bidding?*, IRISH COUNCIL FOR CIVIL LIBERTIES, https://www.iccl.ie/what-is-real-time-bidding/ [https://perma.cc/UAQ5-FTY8] ("What is Real Time Bidding? It's the biggest illegal data breach ever recorded.").

[15] *Glossary*, THE TRADE DESK, https://www.thetradedesk.com/glossary#terms-s [https://perma.cc/E6QV-B4QY].

to multiple demand side platforms ("DSPs"). A DSP is an operation that solicits, processes, and furthers bidding by an advertiser to target a specific consumer with an ad on a website or an app. During the RTB process, DSPs analyze the bidstream data to decide whether to bid for ad space for that user on behalf of their advertiser clients. Even DSPs that lose the RTB auction benefit by collecting user data, which can be added to existing user profiles.

71. The RTB process occurs *178 trillion* times annually across the U.S. and Europe and is widely viewed as privacy invasive.[16] RTB exposes users to privacy risks in numerous ways. First, its sheer scope poses a privacy risk because users' personal information is broadcast to untold numbers of RTB participants. Second, users' data is collected and shared by multiple parties without their consent or control. Third, users are exposed to harmful or misleading ads because the RTB process enables targeting based on sensitive or inaccurate criteria, such as political affiliation, health status, or financial situation.

72. Trade Desk "is the largest independent [DSP] in the world, competing against DoubleClick by Google, Facebook Ads, and others."[17] As a DSP, Trade Desk's role in the RTB ecosystem is to "help[] advertisers buy ads through real-time bidding exchanges"[18] Trade Desk uses its proprietary technology and algorithms to analyze the vast amount of information it tracks and collects about users, and to bid on its clients' behalf for the most valuable ad impressions in real time. By offering these services and platforms, Trade Desk plays a central role in enabling and profiting from the RTB ecosystem. However, by doing so, Trade Desk also exposes users to invasive and pervasive surveillance, profiling, and targeting, without their consent or knowledge.

73. Trade Desk operates behind the scenes, creating identifiers and collecting data from other sources without any consent from or contract with the user. Trade Desk thus faces no direct market pressure to respect consumers' privacy preferences, since it does not depend on their trust or loyalty.

---

[16] *Action File: RTB online ad auctions*, IRISH COUNCIL FOR CIVIL LIBERTIES, https://www.iccl.ie/rtb/ [https://perma.cc/9V45-EKKE].

[17] Wikipedia, *The Trade Desk*, https://en.wikipedia.org/wiki/The_Trade_Desk [https://perma.cc/3V2L-5Y7X].

[18] *Glossary*, THE TRADE DESK, https://www.thetradedesk.com/glossary#terms-d [https://perma.cc/TY32-WGSV].

B. Trade Desk Creates Persistent Deterministic Identifiers as the Foundation for Its Surveillance of Plaintiffs.

74. Instead of interacting with consumers directly, Trade Desk partners with over 350 different entities to obtain these companies' vast stores of user data. Trade Desk partners with companies that trade in data that spans the spectrum of individuals' everyday lives, from some of the largest data brokers and data aggregators in the world (*e.g.*, LiveRamp, Lotame, Acxiom), financial reporting companies (*e.g.*, Equifax, Experian, MasterCard, Visa, Alliant, TransUnion), health and medical data brokers (*e.g.*, Health Link Dimensions, Health Rankings by Symphony Health, Medicx Health, Med Data Group), retailers and pharmacies (*e.g.*, Walmart, Walgreens, Rakuten Insight), to home devices like connected TVs (*e.g.*, Roku).[19]

1. Trade Desk Permanently Brands and Tracks Plaintiffs and Class Members with Its "Unified ID 2.0" Identification Number.

75. Trade Desk leverages the data collected about individuals via its various tracking technologies and data partnerships through its Unified ID 2.0 ("UID2"). UID2 is an identifier that can distinguish between individuals down to the household and individual level.[20] What makes UID2 unique is that it is derived, in part, directly from *deterministic* identifiers,[21] such as an individual's email address and phone number.

76. UID2 is effectively an identity anchor on which Trade Desk can map additional information and continually perfect its "identity resolution" services. "Identity resolution" refers to the process of merging or resolving various distinct data points or touchpoints (an email address and a mobile device ID (or "MAID"), for example) into a comprehensive identity profile of a single person.[22]

---

[19] *Our Partners*, THE TRADE DESK, https://www.thetradedesk.com/us/our-platform/our-partners/partner-directory [https://perma.cc/5GB2-FPPL].

[20] *Unified ID 2.0*, THE TRADE DESK, https://www.thetradedesk.com/us/about-us/industry-initiatives/unified-id-solution-2-0 [https://perma.cc/2XXH-9B83].

[21] Kate Kaye, *WTF is the difference between deterministic and probabilistic identity data?*, DIGIDAY (Apr. 1, 2021), https://digiday.com/media/wtf-is-the-difference-between-deterministic-and-probabilistic-identity-data/ [https://perma.cc/E3V9-NHFX]. ("Deterministic data is information that is known to be true and accurate because it is supplied by people directly or is personally identifiable, such as names or email addresses.").

[22] *How Identity Graphs are Built–The Present and The Future*, THE TRADE DESK, https://www.thetradedesk.com/us/resource-desk/how-identity-graphs-are-built-the-present-and-

77. The assignment and use of UID2 works as follows. Trade Desk obtains a person's email or phone number from one of its partners, along with other information identifying that person's device and interactions with the partner.[23] Once Trade Desk obtains this information, it checks its existing database for whether it has a pre-existing UID2 assigned to that email address or phone number.[24] If a match exists, Trade Desk associates the data it received with the existing UID2 and other user information Trade Desk has about that individual.[25] If a UID2 has not been assigned to that email address or phone number, Trade Desk assigns a UID2 to that user. Thus, the next time the Trade Desk receives the same email address or phone number, it can associate that user and their data with the same UID2.[26]

78. The UID2 is keyed, in part, to a user's email or phone number. That feature effectively allows Trade Desk to track the user's activity when they are logged in to a particular account, *e.g.*, email account, subscription account, mobile app, or Internet-connected TV ("CTV").

79. Trade Desk then leverages that information to identify the same individual across multiple devices, irrespective of their logged-in status on those other devices.[27] In other words, UID2 uses data collected from an individual's "logged in" online activity to identify that same individual across devices, whether they are logged in or logged out and regardless of where they are on the Internet.

80. This cross-device identification extends to Internet-connected televisions ("CTVs"), as well, thus extending Trade Desk's identification systems from desktop computers and mobile devices to the televisions inside people's bedrooms (see depiction below):[28]

---

the-future [https://perma.cc/X29N-TLXF].

[23] *Unified ID 2.0 Overview*, UNIFIED ID 2.0, https://unifiedid.com/docs/intro [https://perma.cc/XDY8-M394].

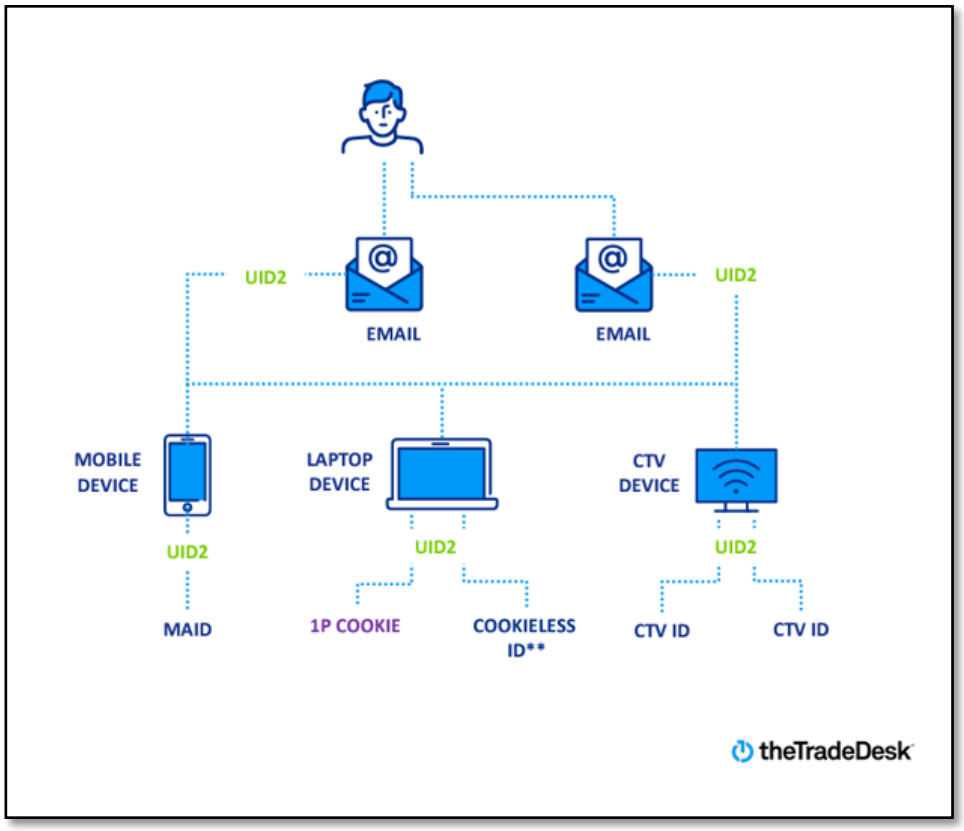
[24] *Frequently Asked Questions*, UNIFIED ID 2.0, https://unifiedid.com/docs/getting-started/gs-faqs#how-should-i-generate-the-sha-256-of-dhttps://unifiedid.com/docs/getting-started/gs-faqs#how-should-i-generate-the-sha-256-of-dii-for-mappingii-for-mapping [https://perma.cc/9CD7-S4D2].

[25] *Id.*

[26] *Id.*

[27] *Unified ID 2.0 Overview*, UNIFIED ID 2.0, https://unifiedid.com/docs/intro [https://perma.cc/XDY8-M394].

[28] Jaime Nash, Director of Product Marketing The Trade Desk, Future Proofing Your Identity



81. Notably, UID2 is a ***stronger*** identifier than those that previously existed, including those that Apple and Google have announced they will deprecate as privacy-invasive. Not only does it reach beyond web browsers and phones, but because UID2 is tied to email addresses and phone numbers[29]—unique personal information that is essentially permanent—it cannot be reset, like traditional advertising identifiers, and does not expire, like cookies.

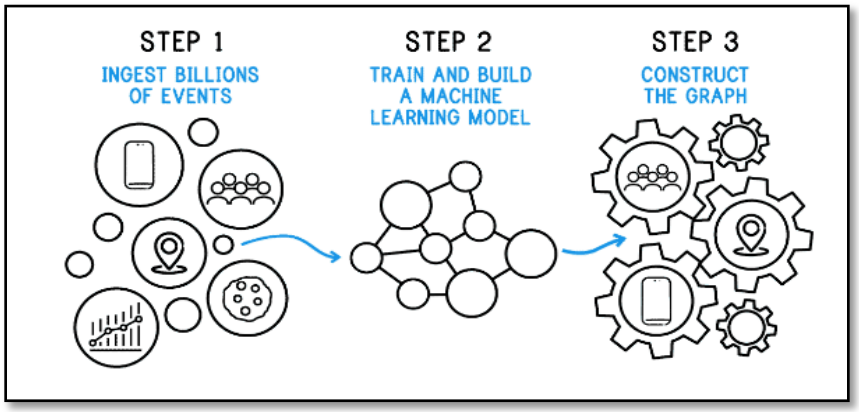
2. Trade Desk Shares and Trades in Surveillance with Other Privacy-Invasive Actors Through Its "Identity Alliance."

82. Trade Desk partners with other privacy-invasive companies that engage in pervasive surveillance in order to fuel the accuracy of its "Identity Alliance."

Strategies, AdExchanger's Programmatic IQ (May 16, 2023); *The new identity era is here*, THE TRADE DESK, https://www.thetradedesk.com/resources/why-advertisers-dont-need-to-rely-on-cookies-video [https://perma.cc/L5JX-STHT].

[29] *How Identity Graphs are Built–The Present and The Future*, THE TRADE DESK, https://www.thetradedesk.com/us/resource-desk/how-identity-graphs-are-built-the-present-and-the-future [https://perma.cc/X29N-TLXF].

83. Identity Alliance is an identity resolution system that combines available cross-device identifiers into an "identity graph."[30] As depicted below, "[i]dentity graphs, like the ones used by [Trade Desk's] Identity Alliance, are essentially built in three steps. They are composed of deterministic identifiers" [*e.g.*, cookies, mobile ad IDs, CTV IDs, hashed emails, UID2, and IP addresses] and "probabilistic" signals [*e.g.*, wifi address, time stamp, geolocation, browser attributes, device attributes, user agent, and contextual data] data to cluster IDs at the household and individual level.[31]



84. While there are various purveyors of "identity graphs," Trade Desk's Identity Alliance is distinguishable because it combines its own identity graph (the "AdBrain" device graph) with identity graphs from other vendors.[32] This "unified graph" thus presents a comprehensive picture of each Class member and their associated devices. As Trade Desk explains: "Identity Alliance maps connections between users and their devices across the device graphs of industry-

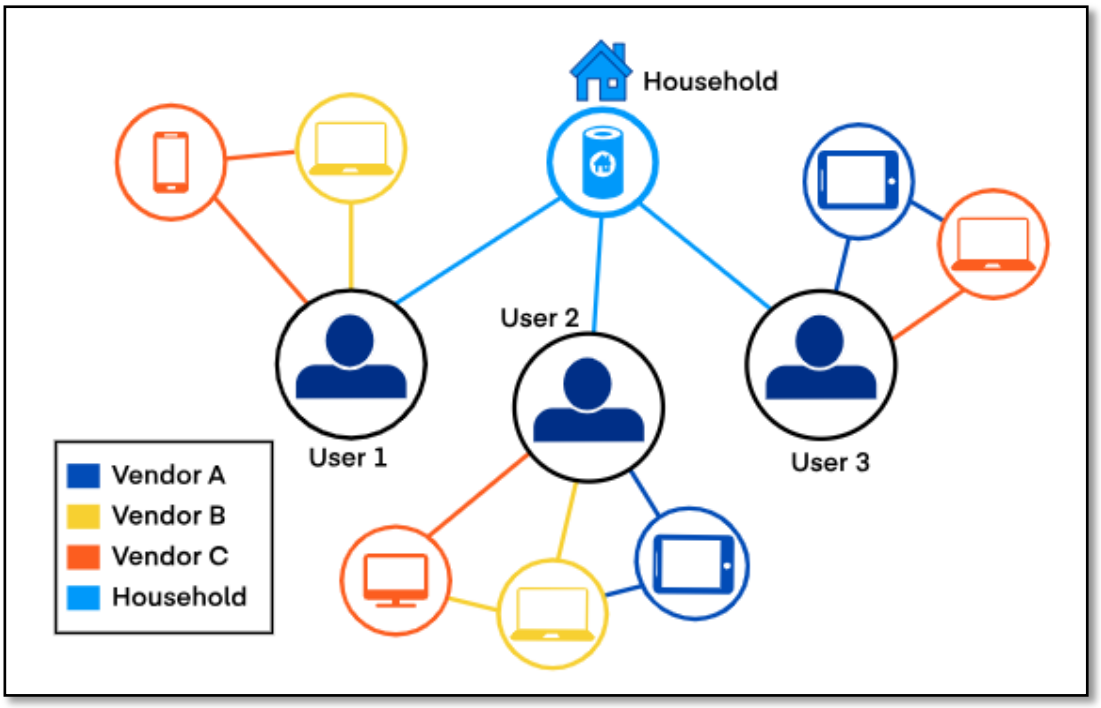
---

[30] *How Identity Graphs are Built–The Present and The Future*, THE TRADE DESK (Mar. 6, 2024), https://www.thetradedesk.com/us/resource-desk/how-identity-graphs-are-built-the-present-and-the-future [https://perma.cc/X29N-TLXF].

[31] *Cross-Device Targeting*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/api/doc/CrossDeviceTargeting [https://perma.cc/PHC5-QSKM].

[32] *How identity graphs are built — the present and the future*, THE TRADE DESK (Mar. 6, 2024), https://www.thetradedesk.com/resources/how-identity-graphs-are-built-the-present-and-the-future [https://perma.cc/G4KR-A37Y]; ADBRAIN, http://www.adbrain.com/ [https://perma.cc/77ML-CWE2]; *The Trade Desk Snaps Up Adbrain As Ad Tech Pursues Cross-Device Roots*, ADEXCHANGER (Oct. 26, 2017), https://www.adexchanger.com/online-advertising/trade-desk-snaps-adbrain-ad-tech-pursues-cross-device-roots/ [https://perma.cc/4PD7-ZEZH].

leading cross-device vendors. For example, the following image illustrates how three vendors A, B, and C might be linked differently to the devices of users 1, 2, and 3 in the same household."[33]



85. According to Trade Desk, "[w]ith this unified graph, your targeting works from a more complete picture of each user's devices."[34] Further, "[a]n additional householder layer connects individuals in a household with the devices that they share, such as a connected television or smart speaker."[35]

86. The below table, taken from Trade Desk's website, shows the various identity graphs that fed and augmented the Identity Alliance. Notably, both LiveRamp and Oracle have been repeatedly accused of violating Internet users' privacy through the creation of their own highly invasive identity graphs,[36] which fed into and augmented Trade Desk's, thereby concentrating and magnifying the privacy invasive-nature of each company's independent activities:

---

[33] *Cross-Device Targeting*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/api/doc/CrossDeviceTargeting [https://perma.cc/PHC5-QSKM].

[34] *Id.*

[35] *Id.*

[36] *See, e.g.*, Wolfie Christl, *Corporate Surveillance in Everyday Life*, Cracked Labs (June 2017),

Vendor Name	Vendor ID	Region	Scale	Accuracy	Supported ID Type
Identity Alliance	10 (person) 11 (household)	US, Canada, EMEA, APAC	Highest	High	Cookies, MAIDs, UID2s, CTV IDs, RampIDs
Adbrain Device Graph	1 (person) 8 (household)	US, Canada, EMEA, APAC	Highest	High	Cookies, MAIDs, UID2s, CTV IDs
Tapad Device Graph	4	US, Canada, APAC	High	High	Cookies, MAIDs, UID2s, CTV IDs
LiveRamp IdentityLink	6	US, UK, France	Low	High	Cookies, MAIDs, RampIDs
Oracle Cross Device	2	US, APAC	Medium	High	Cookies, MAIDs, UID2s

C. Trade Desk's Direct Methods for Collecting Individuals' Personal Information

87. As noted above, the success of Trade Desk's business depends on the accumulation of vast amounts of personal information for as many people as possible. In addition to persistent deterministic identifiers including UID2, Trade Desk uses the following tools to enhance the personal information associated with those identifiers and create detailed dossiers on class members: cookies and cookie syncing, pixels, and its "Real-Time Conversion Events" SDK (discussed below).

https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf; *Katz-Lacabe et al. v. Oracle America, Inc.*, No. 3:22-cv-4792 (N.D. Cal.); *Riganian et al. v. LiveRamp Holdings, Inc. et al.*, No. 4:25-cv-824 (N.D. Cal.). Oracle is no longer listed, having shuttered its own ID Graph after being sued by privacy advocates.

2. Cookies and Cookie Syncing

88. **Cookies:** Trade Desk deploys tracking cookies to follow users across the web. Cookies are pieces of software code placed by Trade Desk and stored on a user's web browser. Cookies allow Trade Desk to "distinguish between, recognize, and store data about unique web browsers and devices, and to store data on [Trade Desk's] servers[.]"[37] The cookies further allow Trade Desk to "recognize web browsers across sites and over time, and therefore to record information about them over time."[38] Trade Desk cookies store and cause the transmission of a unique identifier that enables Trade Desk (and other entities with access to the cookies) to track users as they navigate the website, and any subsequent website where the cookies appear.

89. **Cookie Syncing:** Trade Desk explains to its clients (*e.g.*, advertisers) that cookie syncing (also known as cookie matching or cookie mapping) is "a process of establishing the correlation between unique identifiers (IDs) for the same user" between Trade Desk and its clients.[39] In other words, it is the process of mapping your unique cookie ID for a user to the Trade Desk cookie ID for the same user.[40] Cookie syncing works as follows. A website uniquely identifies a person with an identifier (for example "1234"). Trade Desk uniquely identifies the same person with a different identifier (for example "5678"). Then, Trade Desk obtains the website's identifier for that person so that Trade Desk now knows that its user 5678 is called 1234 by the website—and vice versa. In addition to the website, Trade Desk cookie syncs with other tracking companies. This syncing process is not a one-way street: Trade Desk reaps the benefits as well and is able to match its cookie IDs to its clients' cookie IDs.[41]

---

[37] *Privacy and The Trade Desk Platform*, THE TRADE DESK, https://www.thetradedesk.com/us/privacy#The_Data_Platform_Collects [https://perma.cc/D3QP-F7MW].

[38] *Id.*

[39] *Cookie Mapping*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/data/doc/CookieSyncing [https://perma.cc/38W9-JCGE].

[40] *Id.*

[41] *Privacy and The Trade Desk Platform*, THE TRADE DESK, https://www.thetradedesk.com/us/privacy#The_Data_Platform_Collects [https://perma.cc/D3QP-F7MW] (emphasis added).

90. By engaging in cookie syncing, Trade Desk can map its cookie IDs to other identifiers (used by third parties) and enable other tracking companies to engage in similar activity.

91. Trade Desk engages in cookie syncing through at least two Trade Desk tracking technologies: (i) the Trade Desk Universal Pixel (discussed below), and (ii) the Trade Desk Match Tag. With respect to the latter, when the Trade Desk Match Tag is present on a webpage it will cause the transmission of information to the domain "match.adsrvr.org." That transmission will include the unique cookie ID assigned by Trade Desk for the individual (ttd_id), the unique user ID that is assigned by the Trade Desk client (ttd_puid), and the domain where the cookie synchronization was initiated, *e.g.*, the domain that the user is visiting at the time of cookie syncing.

92. Using its data processing systems, Trade Desk uses the data gathered through Trade Desk cookies, and the cross-correlation provided by cookie matching, to build and refine user profiles and user identification.

93. Trade Desk places cookies and engages in cookie syncing through the placement of source code, which is not visible to users when they are viewing, interacting with, or navigating a website.

3. Universal Pixel (JavaScript)

94. Trade Desk's Universal Pixel is a JavaScript tracking tag that captures and transmits information as an individual navigates through webpages on which the tag is present. The Universal Pixel is designed to gather information about Internet users' activities and interactions with a website, such as actions taken, products viewed, purchase intent, ad conversions (*e.g.*, when a user interacts with a specific ad), and other content communications taken on websites.

95. When someone visits a website where the Universal Pixel is present, Trade Desk receives, at minimum:

a. The content of the user's communication, including but not limited to: the user's email address; the precise URL being viewed by the user; the referrer URL; information regarding actions being taken by the user; purchase content and pricing; and the contents of search queries;

b. The IP address of the user's computer;

c. The precise date and time of the website visit;

d. Unique device identifiers;

e. "User-Agent" (information regarding the specific device being used); and

f. Information about the user's location.

96. Trade Desk provides the following examples of content that may be transmitted to Trade Desk via the Universal Pixel:[42]

```
<script src="https://js.adsrvr.org/up_loader.1.1.0.js" type="text/javascript"></script>
<script type="text/javascript">
    ttd_dom_ready( function() {
        if (typeof TTDUniversalPixelApi === 'function') {
            var universalPixelApi = new TTDUniversalPixelApi();
            universalPixelApi.init("rt7ftg2", ["ejs57s6"], "https://insight.adsrvr.org/track/up",
            {
                "orderid": "abc123XyZ",
                "v": 12.99,
                "vf": "USD",
                "td1": "AlbumName",
                "td2": "Artist",
                "td3": "Genre",
                "td4": "DigitalDownload",
                "td5": "new_customer",
                "dpop": "LDU",
                "dpor": "US-CO"
            });
        }
    });
</script>
```

Trade Desk example illustrating the Universal Pixel's interception of content information related to the user's purchase of an album, which includes the price, currency, album name, artist, genre, purchase location and whether this is a "new customer"

97. In addition, Trade Desk's Universal Pixel is designed to *always enable* cookie syncing (described above) so that it cannot be turned off.[43]

98. Trade Desk implements the Universal Pixel through the placement of source code. It is not visible to users when they are viewing, interacting with, or navigating a website.

[42] *Universal Pixel*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/data/doc/TrackingTagsUniversalPixel [https://perma.cc/8PPM-BZMT].

[43] *Id.*

4. Static Tracking Pixels

99. Similar to cookies and the Universal Pixel, static tracking pixels are pieces of code that are embedded onto webpages. Static tracking pixels are not visible to users when they are viewing, interacting with, or navigating a website or mobile application. According to Trade Desk, its static tracking pixels track and pass back to Trade Desk information about pages visited and user actions taken on a given page. "[T]racking tags can pass information about pages visited or user actions taken on a given page, such as pressing buttons or making selections. For example, placing a pixel on a home page would track users who visit the page. Placing a tag on an order confirmation page can track users who purchased something[.]"[44]

100. When a user visits a website where Trade Desk's static tracking pixels are present, the user's information will be intercepted and transmitted to Trade Desk's tracking domain, adsrvr.org, and will include, at minimum:

a. The content of the user's communication, including but not limited to: the precise URL being viewed by the user; the referrer URL; information regarding actions being taken by the user; purchase pricing and content; and the contents of search queries;

b. The IP address of the user's computer;

c. The precise date and time of the website visit;

d. Unique device identifiers;

e. User-Agent (information regarding the specific device being used); and

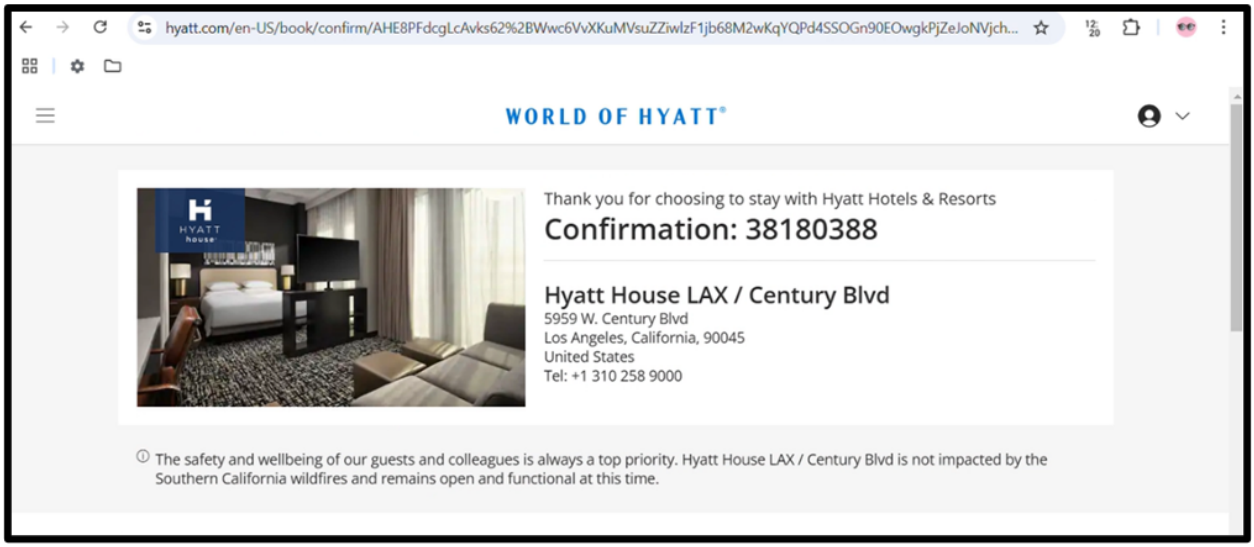
f. Information regarding the user's location.

101. Trade Desk implements the static pixels through the placement of source code. It is not visible to users when they are viewing, interacting with, or navigating a website.

102. The pixels are configured to collect specific information depending on the website. On some websites, like health and booking websites, the pixels intercept the content of the website user's communications with the websites.

[44] *Tracking Tags*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/data/doc/TrackingTagsOverview [https://perma.cc/DXA3-CZRX].

103. For example, the insight.adsrvr.org tracking pixel is loaded onto the Hyatt hotel website. In real time as website visitors select booking options and make reservations, Trade Desk's tracking pixel intercepts the detailed URL from the website, which contains the booking information communicated by the website user to the website, and other information related to the booking.



Adsrvr - Check in details
https://insight.adsrvr.org/track/up?
Tue Feb 11 12:18:39 EST 2025 34 Complete

adv 634adpn
ref
https%3A%2F%2Fwww.hyatt.com%2Fshop%2Frooms%2Flaxxl%3FcheckinDate%3D2025-02-27%26checkoutDate%3D2025-03-02%26rooms%3D1%26adults%3D1%26kids%3D0%26rate%3DStandard%26hpesrId%3Dps__mg0qdvBQaWu9kYS9CQsVrTJJj_vYw6j8
upid l48u72s
upv 1.1.0
td1 Los%20Angeles
td2 US
td3 laxxl
td4 1
td6 3
td8 Hyatt%20House%20LAX%20/%20Century%20Blvd
td9 Hyatt%20House
paapi 1

5. Real Time Conversion Events SDK (Software Development Kit)

104. Trade Desk's "Real Time Conversion Events SDK" is a software development kit that captures and transmits information as an individual interacts with an application or website on which it is integrated.[45] The Real Time Conversion Events SDK is designed to gather information about activities and interactions within an application or website, such as actions taken, product

[45] *Real-Time Conversion Events*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/data/doc/DataConversionEventsApi [https://perma.cc/WY4N-6XZE].

views, purchase intent, ad conversions (*e.g.*, when a user interacts with a specific ad), and other content communications within the application or website.

105. When a user interacts with an application or website where the Real Time Conversion Events SDK is integrated, Trade Desk receives, at minimum:[46]

a. The content of user's communication, including but not limited to: the precise URL or in-app screen being viewed by the user; the referrer URL or previous in-app screen; information regarding actions being taken by the user, such as add-to-cart or purchase events; purchase content and pricing; and the contents of search queries;

b. The IP address of the user's device;

c. The precise date and time of the interaction;

d. Unique device identifiers (such as UID2, TDID, IDFA, AAID, NAID, and DAID);

e. "User-Agent" (information regarding the specific device being used); and

f. Information regarding the user's location.

106. Trade Desk implements the Real Time Conversion Events SDK through the integration of the SDK into the source code of the application or website. It operates in the background and is not visible to users when they are interacting with and navigating the application or website. This seamless integration allows for continuous but surreptitious data collection, without notifying the user that it is happening.

107. By integrating the Real Time Conversion Events SDK, Trade Desk can gather extensive data on user behavior and website interactions.

6. Data Collection Through Trade Desk's Demand Side Platform and Real-Time Bidding

108. As noted above, Trade Desk operates one of the largest "demand side platforms" ("DSPs") in the world. In running its DSP, Trade Desk participates on behalf of advertisers in ad exchanges via the Real Time Bidding ("RTB") process to place advertisements on "publishers'" web properties. Trade Desk is also able to obtain and store the information contained in bid

[46] *Id*.

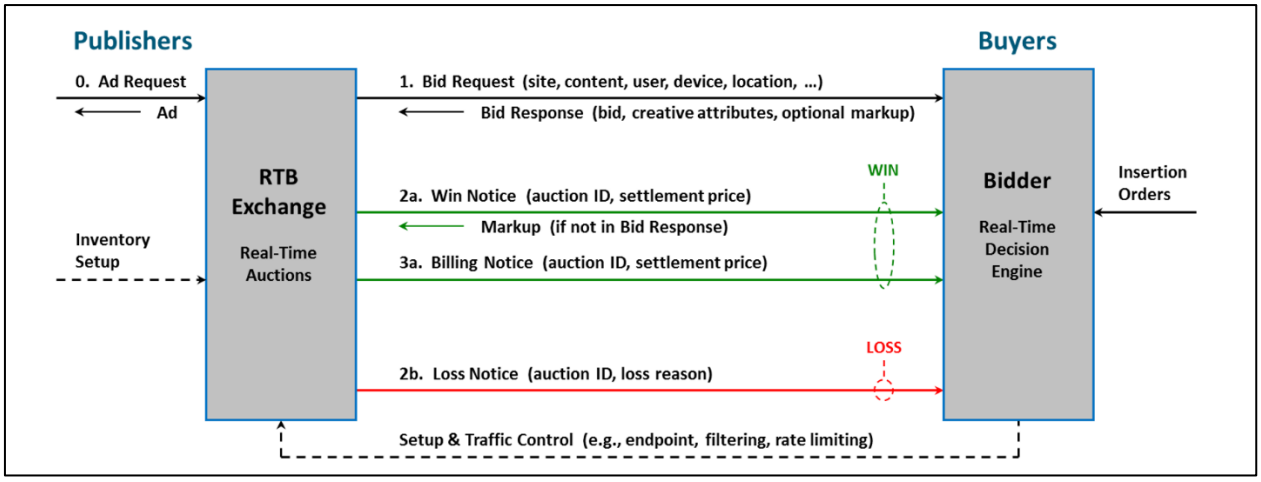
requests[47]—including information regarding individuals' unique identifiers, location information, and browsing history—to further augment its coffers of user data. Moreover, many ad exchanges also facilitate cookie syncing, thus continuing the inescapable loop of tracking and data mining.

109. According to Trade Desk, its DSP reaches up to *4 billion people per day* and is able to reach the same consumer on every device they use.[48] Given the staggering rate and scale of RTB—billions of bid requests in milliseconds—Trade Desk's data mining through its participation as a DSP is practically limitless.

110. Trade Desk's DSP also collects consumer data as a participant in RTB auctions run by RTB exchanges such as OpenX and Google on at least hundreds of thousands of websites, smartphone apps, and connected television applications.

111. As a participant, Trade Desk collects data that includes information about the site, content, user, device, location, and more involved in the communication.[49]

112. The process is illustrated and explained below by a leading industry group that sets standards for RTB auctions:[50]



[47] An ad space is made available through a bid request, which contains personal information about individuals, including unique identifiers, browsing history, and content of communications. During the RTB process, supply-side platforms send bid requests to demand side platforms.

[48] The Trade Desk, *Programmatic Principles: Intro to Programmatic*, YOUTUBE at 5:10 (June 20, 2018), https://www.youtube.com/watch?v=VqfaIgU3fd8.

[49] *About the IAB Tech Lab*, GITHUB, https://github.com/InteractiveAdvertisingBureau/openrtb2.x/blob/main/2.6.md [https://perma.cc/PC9E-YMJX].

[50] *Real Time Bidding (RTB) Project OpenRTB API Specification Version 2.5*, IAB (Dec. 2016), https://www.iab.com/wp-content/uploads/2016/03/OpenRTB-API-Specification-Version-2-5-

113. The full set of information that Trade Desk collects through RTB is set forth in the RTB protocol published by the Interactive Advertising Bureau.[51] The information includes: identifiers and identifiable information in the form of (1) IP address; (2) user agent; and (3) device properties such as screen width, screen height, language, connection type; and (4) identifiers such as Trade Desk's cookie (TDID) and Unified ID, as well as proprietary identifiers from Trade Desk's partners such as LiveRamp, ID5, Pubmatic, and OpenX. The information also includes communications content in the form of (1) the domain or app involved in the communication; (2) the content categories of (a) the site, app, and publisher (b) current sections of the site or app, and (c) the current page or view of the site or app; (3) the "URL of the page;" (4) the "referrer URL that caused navigation to the current page;" (5) the "search string that caused navigation to the current page;" (6) details about the publisher and content with the site or app; (7) keywords about the site or app; (8) the title of the video or article, such as "A New Hope" for a movie or "Why an Antarctic Glacier is Melting So Quickly" for a Time magazine article; (9), the "series" of the content, for example, "The Office" for a television show, or the name of a blog associated with a magazine; (10) the season of the show; (11) the artist credited with the content; (12) the genre of the content and categories describing it; (13) the URL of the content and categories assigned to it; and (14) keywords describing the content.[52]

114. This detailed personal information collected through the RTB process is then associated with the dossier Trade Desk maintains on Plaintiffs and Class members, as illustrated by the "BidFeedback Results" Excel sheet that Trade Desk provided to Plaintiffs Michie and Ju.

D. Trade Desk Uses the Vast Amounts of Data It Collects from Class Members to Create Cradle-to-Grave Dossiers on Them.

115. Trade Desk leverages the data collected about individuals via its various tracking technologies and data partnerships to fuel its "audience" creation. An "audience" is a specific

FINAL.pdf.

[51] *About the IAB Tech Lab*, GITHUB, https://github.com/InteractiveAdvertisingBureau/openrtb2.x/blob/main/2.6.md [https://perma.cc/PC9E-YMJX].

[52] *Id*.

person or group of people that is or are the target of an advertising campaign. When combined with persistent identifiers such as UID2, the collection of "audiences" a person has been placed in can reveal highly specific facts about that person and intimate details about their daily lives.

116. Audiences are made up of data elements, *i.e.*, "segments" of information that come from first-party data or third-party data sources.[53] First-party data elements are segments that a company owns and is sending to Trade Desk.[54] When a company uploads its first-party data, Trade Desk's systems ingest and parse that information to assist in the creation of audiences and targeted advertising. Third-party data elements are segments that data providers have sent to Trade Desk and are available for purchase by Trade Desk's partners, for use in "audience targeting" and other forms of manipulation.[55]

117. By Trade Desk's own admission, many segments made available for sale by Trade Desk are based on sensitive data "related to [Plaintiffs' and Class members] health, such as information on certain past, present, or future medical conditions, and information about race, ethnicity, sexual orientation, or religion, and precise geolocation information."[56]

118. Trade Desk admits it collects, compiles, and uses virtually all electronically trackable information about Plaintiffs and Class members, including all of the following:

> [I]dentifiers (such as cookie identifiers, mobile device advertising identifiers, pseudonymous identifiers derived from email address or phone numbers, IP address, or hashed email address), Internet or other electronic network activity information (such as information about sites [Class members] visit), geolocation data (which may include precise geolocation information), inferences we may make about [Class members'] interests (such as the personalised profiles described above), and data that may reveal demographic information or inferences about gender, race, ethnicity, religion, health, or sex life or sexual orientation.[57]

---

[53] *Audiences*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/api/doc/Audience [https://perma.cc/TGX3-7W5W].

[54] *Id.*

[55] *Id.*

[56] *Privacy and The Trade Desk Platform*, THE TRADE DESK, https://www.thetradedesk.com/legal/privacy [https://perma.cc/D3QP-F7MW].

[57] *Id.*

119. Health-related segments include, for example, "sexuality," "calorie counters," UTIs, smoking cessation, osteoarthritis, macular degeneration, constipation, reproductive health, asthma, auto-immune diseases of the skin, and "joint pain sufferers".[58]

120. Trade Desk's political segments are equally extensive, intrusive, bi-partisan, and cross-ideological. They track, among other things, LGBTQ donors and supporters, marriage equality opposition, environmentalists, abortion, gun rights advocates, protest movement supporters, marijuana legalization advocates, conservative couples, politically divided households, critics of President Trump, Hispanic democrats, "left out democrats," "bible belt conservatives," and political activists, among other political categories.[59]

121. Trade Desk further admits that it creates "personalised profiles" of Class members by associating the information it has on them with identifiers and interest segments.[60] Trade Desk's privacy disclosures misleadingly suggest that these profiles are largely benign, containing "common interests or characteristics, such as "clothing," "sports," "travel," "male," "25-54," and so on."[61] However, as described in detail above, the "personalised profiles" Trade Desk has compiled on Plaintiffs demonstrate that these electronic dossiers actually contain highly sensitive health, political and sexual activity information, comprising *tens of thousands* of individual data points about Plaintiffs.

122. These "personalized profiles" additionally include *inferences* related to class members that are derived from their personal data. For example, Trade Desk admits that it "collects and process[es]" "interest information inferred by us from web browsing history."[62] It does this in part through its "Inferred Brand Intent (IBI)" product offering, which analyzes keywords in the

---

[58] *Health Segments*, THE TRADE DESK, https://www.thetradedesk.com/assets/global/documents/HealthSegments_PrivacyPolicy_210208_164431.pdf [https://perma.cc/8ERC-PGDC].

[59] *NAI Political Segments*, THE TRADE DESK, https://www.thetradedesk.com/assets/global/documents/NAI_PoliticalSegments_PrivacyPolicy.pdf [https://perma.cc/WS3H-HLTS].

[60] *Privacy and The Trade Desk Platform*, THE TRADE DESK, https://www.thetradedesk.com/legal/privacy [https://perma.cc/D3QP-F7MW].

[61] *Id.*

[62] *Id.*

URLs Class members browse to infer their interests.[63] Such inferences, when based on personal information, themselves becomes personal information.[64] Trade Desk further creates detailed inferences about Class members through its "Audience Predictor" product, which uses "proprietary targeting algorithms" to infer traits like political views based on seemingly unrelated data points, such as the type of car they drive, whether they chew gum, and whether they prefer hunting or fishing.[65] The California Attorney General has recognized that such "seemingly innocuous data points, when combined with other data points across masses of data, may be exploited to deduce startlingly personal characteristics," and that "once a business has made an inference about a consumer, the inference becomes personal information—one more item in the bundle of information that can be bought, sold, traded, and exploited beyond the consumer's power of control."[66]

123. As described above, the dossiers Trade Desk created on Plaintiffs Michie, Dyer, and Ju each consist of *tens of thousands* of segments that reflect highly specific and sensitive information about Plaintiffs such as their health conditions, political views, and sexual activities. On information and belief, Trade Desk collected this data about Plaintiffs from hundreds of "Audience Data Providers," as described below.

E. Trade Desk Leverages the Data Collected About Individuals Via Its Various Tracking Technologies and Data Partnerships to Fuel Its Demand Side Platform for Use in Real-Time Bidding.

124. As a DSP, Trade Desk bids on ad space on behalf of advertisers.[67] Importantly, part of the reason Trade Desk is so successful as a DSP—and why it can obtain so much data through this process—is because of its role as creator and operator of the UID2. Many publishers, *i.e.*, the

---

[63] *Connect your ads to audience online browsing behavior with Inferred Brand Intent*, THE TRADE DESK, https://www.thetradedesk.com/resources/connect-your-ads-to-audience-online-browsing-behavior-with-inferred-brand-intent.

[64] 105 Ops. Cal. Att'y Gen. 26 (2022), 2022 WL 815641, at * 2 ("inferences" such as segments constitute personal information).

[65] *Making History: Programmatic in Politics*, THE TRADE DESK, at 14, https://democraticmedia.org/assets/resources/the_trade_desk_election2016_mar163.pdf [https://perma.cc/WA6L-397D].

[66] 105 Ops. Cal. Att'y Gen. 26 (2022), 2022 WL 815641, at * 2.

[67] *Glossary*, THE TRADE DESK, https://www.thetradedesk.com/glossary#terms-d [https://perma.cc/TY32-WGSV].

entities offering the ad space, *themselves* use UID2 and Trade Desk's services. When these publishers seek to offer ad space on their web properties, they include UID2, among other data, in the bid request. As Trade Desk already has individualized dossiers for each user associated with a UID2, Trade Desk has an advantage over other DSPs because it knows precisely who will see the ad, alongside their existing activity and behaviors. Thus, Trade Desk is uniquely situated by virtue of its dual role—as UID2 operator and DSP—which it leverages to successfully facilitate hyper-specific targeting on behalf of its clients for profit.

125. Trade Desk acts as the "ID Operator," receiving email addresses and other personally identifiable information from the publisher and, in return, transmits the UID2. When that publisher later makes a bid request, it includes UID2 in the bid. Trade Desk, then acting as DSP, uses the existing user profile associated with that UID2 to inform its bid strategy.[68]

126. Trade Desk offers advertisers additional ways to maximize Trade Desk's individually identifiable profiles and their bid request. For instance, advertisers that use Trade Desk's DSP can set up an ad campaign and identify specific parameters for ad placement. For example, the advertiser may seek to target certain audiences.[69] Audiences can be based on any number of factors, including interests, location, demographics, and specific device platforms (*e.g.*, CTV, mobile device, etc.).

127. As the DSP, Trade Desk's job is to ensure that any bids it places on behalf of the advertiser fall within the specified audiences. Trade Desk does so by utilizing its vast data profiles on individuals. Trade Desk is able to leverage the full breadth of personal information collected—via online tracking, data partnerships, and offline collection—to make real-time recommendations and bids to ensure accurately targeted advertising.

128. Trade Desk's DSP functions in part as an online store owned and operated by Trade Desk. Trade Desk facilitates the buying and selling of data and data-derived services by Trade Desk

---

[68] *Unified ID 2.0 Overview*, UNIFIED ID 2.0, https://itega.org/wp-content/uploads/2021/01/Trade-Desk-UID2-Overview-Dec-2020.pdf.

[69] *Audience Targeting*, THE TRADE DESK, https://www.thetradedesk.com/our-demand-side-platform/audience-targeting [https://perma.cc/V9BZ-YY2T].

and its so-called "Partners" to private commercial entities and political campaigns. Trade Desk's DSP allows the confluence of mass amounts of personal information by which its participants, including Trade Desk, can continually track people's activities and enrich people's dossiers. Trade Desk describes this as its "data marketplace."[70]

129. Trade Desk's data marketplace is an online market trading in the sensitive and private personal information of tens of millions of people, through which it sells third-party data.[71] Trade Desk describes this massive personal information bazaar as enabling advertising participants to "[d]iscover and target [their] most relevant audiences using behavioral, demographic, and interest signals from leading data providers."[72]

130. The data marketplace is integrated into Trade Desk's broader "Data Management Platform" ("DMP").[73] Through its DMP, Trade Desk "[c]ollects, processes, and stores large amounts of audience data such as cookie IDs, first-party data, and third-party data . . . to better target online ads at specific audiences on a given website."[74]

131. An advertiser accesses the data marketplace by selecting third-party segments when creating audiences for ad campaigns. When an advertising bid is placed based on a third-party segment, the third-party data partner gets a percentage cut of the bid.

132. Trade Desk collaborates with dozens of major third-party data brokers and refers to these companies as "Partners."[75] Trade Desk specifically denotes Partners who want to sell their third-party "ID-based data" segments as "Audience Data Providers."[76] To sell third-party segments

---

[70] *Glossary*, THE TRADE DESK, https://www.thetradedesk.com/glossary#terms-d [https://perma.cc/TY32-WGSV].

[71] Trade Desk Inc. Investor Day, Fair Disclosure Wire (Oct. 4, 2022).

[72] *Audience Targeting: Put your audience at the center of your strategy*, THE TRADE DESK, https://www.thetradedesk.com/us/our-platform/audience-targeting [https://perma.cc/V9BZ-YY2T].

[73] *Third-Party Data Rates*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/data/doc/DataRatesOverview [https://perma.cc/8J2B-LRXJ] ("In the data management platform (DMP), buyers can filter segments . . . .").

[74] *Glossary*, The Trade Desk, https://www.thetradedesk.com/glossary#terms-d [https://perma.cc/TY32-WGSV].

[75] *Our Partners*, THE TRADE DESK, https://www.thetradedesk.com/us/our-platform/our-partners/partner-directory [https://perma.cc/5GB2-FPPL].

[76] *Getting Started for Audience Data Providers*, THE TRADE DESK PARTNER PORTAL,

on Trade Desk's data marketplace, Partners must organize the data segments into a taxonomy and upload the data to Trade Desk's DMP.[77] For segments based on a person's email address or phone number, the Audience Data Provider must first convert the personal identifier to a unified ID for assimilation into Trade Desk's massive identity graph.[78]

133. Once Audience Data Providers have uploaded their "inventory" to the DMP, they can then choose to make their third-party data segments available to all buyers in the platform ("syndicated" segments) or only to certain specified advertisers ("custom" segments).[79]

134. The personal information sold by Audience Data Providers on Trade Desk's data marketplace can be used to enhance the digital dossiers in Trade Desk's systems. Once uploaded into the DMP, this data becomes available for sale to Trade Desk's advertising clients through its DSP to enrich the data they have on individuals or to fine-tune their targeting for the RTB process.

135. Trade Desk's public-facing documentation for Audience Data Providers does not address privacy concerns beyond noting that Partners must "adhere to our privacy policies"[80] and briefly cautioning that "Trade Desk may reject segments if the DisplayName and Description [data fields] contain terms from sensitive categories. Generally, at this time, the categories that Trade Desk considers sensitive include health conditions, ethnicity, race, religious affiliation, union membership crime victim status, children's data, and sexual orientation."[81] While Trade Desk thus claims to prohibit putting certain sensitive segment data up for sale on its data marketplace, it is impossible to tell whether and how Trade Desk enforces these restrictions. For example, while Trade Desk claims to prohibit segments that "contain terms" from categories such as race, as

---

https://partner.thetradedesk.com/v3/portal/data/doc/DataGetStarted3pProviderAudience [https://perma.cc/6RUL-LPLH].

[77] *Id*.

[78] *Id*.

[79] *Getting Started for Audience Data Providers*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/data/doc/DataGetStarted3pProviderAudience [https://perma.cc/6RUL-LPLH]; *Third-Party Data Rates*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/data/doc/DataRatesOverview [https://perma.cc/8J2B-LRXJ].

[80] *Id*.

[81] *Third-Party Audience Data Segments and Rates*, THE TRADE DESK PARTNER PORTAL, [https://perma.cc/29FM-S2CZ].

demonstrated below, Trade Desk's website lists numerous Audience Data Providers whose entire business model consists of targeting Hispanic audiences (*e.g.*, Retargetly, DataXpand, and Navegg).[82]

136. Many of Trade Desk's Audience Data Providers openly advertise the sale of highly intrusive and offensive personal information:

a. **Mobilewalla:**[83] Boasts of having "billions of data points daily" from 276 million unique mobile devices in the U.S. alone,[84] and 1.5 billion mobile devices in 31 countries worldwide.[85] In particular, Mobilewalla sells age, gender, GPS, and location data. Mobilewalla specifically advertises the personal location information it sells as a way to increase political campaign results.[86] During the summer of 2020, Mobilewalla tracked mobile devices to collect data on 17,000 Black Lives Matter protesters including their home addresses and demographics. Mobilewalla also released a report entitled "George Floyd Protester Demographics: Insights Across 4 Major US Cities," which prompted a letter and investigation by Senator Elizabeth Warren and other congress members.[87] In response to this investigation, Mobilewalla revealed that it had provided location data used by the Department of Homeland Security, the Internal Revenue Service, and the U.S. military for warrantless tracking of devices both at home and abroad.[88] In

---

[82] *Our Partners*, THE TRADE DESK, https://www.thetradedesk.com/us/our-platform/our-partners/partner-directory [https://perma.cc/5GB2-FPPL].

[83] *See* Mobilewalla listed in Trade Desk's Partner Directory, *Our Partners*, THE TRADE DESK, https://www.thetradedesk.com/us/our-platform/our-partners/partner-directory [https://perma.cc/5GB2-FPPL].

[84] *Warren, Maloney, Wyden, DeSaulnier Probe Data Broker's Collection of Data on Black Lives Matter Demonstrators*, House Committee on Oversight and Reform, Chairwoman Carolyn B. Maloney, (Aug. 4, 2020) https://perma.cc/VKW2-NQSK.

[85] *What is Geo-Behavioral Advertising?*, MOBILEWALLA (Feb. 8, 2019), https://www.mobilewalla.com/blog/what-is-geo-behavioral-advertising [https://perma.cc/N9H2-YTRC].

[86] *Audience Segments*, MOBILEWALLA, https://www.mobilewalla.com/products/audience-segments [https://perma.cc/KW4D-H5F7].

[87] John Donegan, *The Incessant Surveillance by Data Brokers Needs to be Addressed*, ManageEngine (Oct. 6, 2021), https://insights.manageengine.com/privacy-compliance/the-incessant-surveillance-by-data-brokers-needs-to-be-addressed/ [https://perma.cc/F8HX-ZPHF].

[88] Bryan Tau, *How Cellphone Data Collected for Advertising Landed at U.S. Government Agencies,* THE WALL STREET JOURNAL (Nov. 18, 2021), https://www.wsj.com/articles/mobilewalla-says-data-it-gathered-from-consumers-cellphones-ended-up-with-government-11637242202 [https://perma.cc/S6AB-93XY].

December 2024, the Federal Trade Commission (FTC) filed a complaint alleging the company unlawfully tracked and sold consumers' sensitive location data, and collected data from RTB advertising exchanges for other purposes.[89] The FTC finalized an order in January 2025 banning Mobilewalla from both such activities.[90]

b. **Unacast (formerly Gravy Analytics):**[91] Advertises location intelligence at "millions of places, points-of-interest and local events" to power "precision-targeted mobile advertising campaigns." Its "Brand Audiences" include 2000-plus U.S. chain locations such as BestBuy, Burger King, Starbucks, and Target.[92] It also sells phone location data to government agencies.[93] Indeed, the FBI contracts with Gravy Analytics' subsidiary, Venntel, for the monitoring of social media posts and location data. In 2020, the House Committee on Oversight and Reform opened an investigation into Venntel for its business of buying location data from various smartphone apps and selling that data to agencies including the FBI, DHS, DEA, ICE, CBP, and the IRS. The Trump Administration also used Gravy Analytics' location data to track people crossing the US-Mexico border. The FTC finalized an order in January 2025 prohibiting Gravy

---

[89] *FTC Takes Action Against Mobilewalla for Collecting and Selling Sensitive Location Data*, FTC (Dec. 3, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-mobilewalla-collecting-selling-sensitive-location-data [https://perma.cc/9UZS-2QJ4].

[90] *FTC Finalizes Order Banning Mobilewalla from Selling Sensitive Location Data*, FTC (Jan. 14, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-order-banning-mobilewalla-selling-sensitive-location-data [https://perma.cc/WC8U-5S97].

[91] *See* Gravy Analytics listed in Trade Desk's Partner Directory, *Our Partners*, THE TRADE DESK, https://www.thetradedesk.com/us/our-platform/our-partners/partner-directory [https://perma.cc/5GB2-FPPL].

[92] *Gravy Analytics Unveils Location Data Forensics*, GRAVY ANALYTICS (Dec. 19, 2018), https://perma.cc/SE3K-KMSH; *Location-Based Advertising: Brand Audiences*, GRAVY ANALYTICS (Mar. 26, 2018), https://perma.cc/4C4B-PSYP; *Paramount, Best Buy & Gravy Analytics: Consumer Insights for Advertising*, GRAVY ANALYTICS, https://perma.cc/E8UU-H6AY; *Starbucks & the Pumpkin Spice Latte: Using Location Data to Measure Foot Traffic*, UNACAST, (Aug. 21, 2019), https://www.unacast.com/post/starbucks-pumpkin-spice-latte-using-location-data-measure-foot-traffic [https://perma.cc/DJ38-JGUU].

[93] Lee Fang, *FBI Expands Ability To Collect Cellphone Location Data, Monitor Social Media, Recent Contracts Show*, The Intercept (June 24, 2020), https://theintercept.com/2020/06/24/fbi-surveillance-social-media-cellphone-dataminr-venntel/ [https://perma.cc/MJ58-QL3Z].

Analytics and Venntel from "unlawfully tracking and selling sensitive location data from users, including data about consumers' visits to health-related locations and places of worship."[94]

c. **Affinity Answers:**[95] Advertises data on Class members' interests in political organizations (*e.g.*, NAACP, National LGBTQ Task Force, Planned Parenthood), political media figures (*e.g.*, Bill O'Reilly, Glenn Beck, Anderson Cooper, Arianna Huffington), state-level Democratic Party and Republican Party organizations, and specific politicians in office.[96] It harvests information about hundreds of millions of users from major social networks such as Facebook, Instagram, and Twitter.

d. **Eyeota:**[97] Dun & Bradstreet subsidiary Eyeota offers a vast range of sensitive categories.[98] These include national security categories described as "People who work in the Navy," "in the Marines," "in the Army," "in the Air Force," "in the Coast Guard," "in the military," "in the Pentagon," "in law enforcement," "in [the] judiciary," "in government," and one for "Elected Officials." Even former service members are targeted; the "Military DoD" category applies to "Professionals who have honorably served or are currently serving in the military."[99]

---

[94] *FTC Finalizes Order Prohibiting Gravy Analytics, Venntel from Selling Sensitive Location Data*, FTC (Jan. 14, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-order-prohibiting-gravy-analytics-venntel-selling-sensitive-location-data [https://perma.cc/3QPP-VBPU].

[95] *See* Affinity Answers listed in Trade Desk's Partner Directory, *Our Partners*, THE TRADE DESK, https://www.thetradedesk.com/us/our-platform/our-partners/partner-directory [https://perma.cc/5GB2-FPPL].

[96] Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals*, DUKE UNIVERSITY Sanford Cyber Policy Program (2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf [https://perma.cc/EL5G-JM52].

[97] *See* Eyeota listed in Trade Desk's Partner Directory, *Our Partners*, THE TRADE DESK https://www.thetradedesk.com/us/our-platform/our-partners/partner-directory [https://perma.cc/5GB2-FPPL].

[98] *Eyeota RTB segment list (global), December 2021*, IRISH COUNCIL FOR CIVIL LIBERTIES (Nov. 17, 2023), https://www.iccl.ie/wp-content/uploads/2023/10/Doc-2-as-printed-Eyeota-8-December-2021.pdf [https://perma.cc/8C8H-L8RS]. The Eyeota category list was originally downloaded on December 8, 2021, and is one of the sources of a recent security report by the Irish Council for Civil Liberties. *America's Hidden Security Crisis*, IRISH COUNCIL FOR CIVIL LIBERTIES (Nov. 14, 2023), https://www.iccl.ie/digital-data/americas-hidden-security-crisis/ [https://perma.cc/EEB5-A4UV].

[99] *Eyeota RTB segment list (global), December 2021*, IRISH COUNCIL FOR CIVIL LIBERTIES (Nov. 17, 2023), https://www.iccl.ie/wp-content/uploads/2023/10/Doc-2-as-printed-Eyeota-8-December-2021.pdf [https://perma.cc/8C8H-L8RS].

Eyeota also provides categories that could be used to influence these individuals, such as "Substance Abuse," "Alcohol," "Gamblers," "Payday Loans," "Debt," and "Welfare and Unemployment."[100] Nor are politics and health off limits. Eyeota offers political categories like "Republican," "Leans Right," "Conservative," "Libertarian," "Eligible Voters," "Likely Voter," "Likely Gun Owners," and "Oppose Raising Taxes." Health categories include "Heart Disease," "Diabetes," "Chronic Pain," "Chronic Fatigue Syndrome," "Sleep Disorders," "Panic / Anxiety Disorders," "Depression," "Psychology / Psychiatry," "Physical Therapy," and "Surgery."[101]

e. **Pogo:** Trade Desk advertises its partnership with Pogo as helping "advertisers trace a more robust consumer story using always-on behavioral data, including basket-level transactions."[102] Pogo touts its ability to record consumers' "every single transaction" down to the item purchased and amount spent, combined with a person's credit score, household income, and how "loyal" a customer they are to specific brands or stores.[103] The company appears to gather data beyond "real-time purchases," including extensive financial data and sensitive health data including "calories, BMI, exercise, and more."[104]

137. On information and belief, these sensitive segments made available by Trade Desk's Audience Data Providers were for sale on Trade Desk's data marketplace.

138. Trade Desk provides, and profits from, this data marketplace that allows third-party data brokers to traffic in Class members' highly sensitive personal information. The following examples non-exhaustively illustrate the types of sensitive information Trade Desk facilitates the sale of through its data marketplace:

---

[100] *Id.*

[101] *Id.*

[102] *3 Ways to Harness Behavioral Data*, THE TRADE DESK, (Mar. 25, 2024) https://www.thetradedesk.com/us/resource-desk/3-ways-to-harness-behavioral-data [https://perma.cc/D3G8-KPL9].

[103] *Eliminate your data blindspots within minutes*, POGO, https://partners.joinpogo.com/ [https://perma.cc/E9VL-KGUN].

[104] *Id.*

a. **Race:** Several data brokers expressly provide racial categories as "audience segments." For example, multiple data brokers' (*e.g.*, Retargetly, DataXpand, and Navegg) business model consists entirely of targeting Hispanic audiences.[105]

b. **Location:** Data brokers such as Mobilewalla, described above, offer location tracking for sale on Trade Desk's data marketplace. For example, TrueData advertises "real-time GPS and beacon location signals" on 245 million U.S. mobile users.[106] Trade Desk also offers its own "geo-interest segments" for CTV product, which allows advertisers to "target co-located people with potentially similar interests."[107]

c. **Politics:** Data brokers participating in Trade Desk's data marketplace purport to offer segments based on detailed political information, and some are avowedly partisan in doing so. i360, for example, bills itself as "a leading data and technology resource for the pro-free-market political and advocacy community" with a database of "220 million voters from all 50 states."[108] It boasts a dataset that includes "extensive political identification, coalition, and membership information collected by way of in-person, phone and online surveys, as well as through partner relationships in addition to lifestyle and consumer data collected from multiple top-tier providers."[109] It advertises registration and partisanship segments such as "Catholic," "Pro 2nd Amendment," "Pro Choice," "Pro Life," "Pro Marriage Same Sex," "Pro Traditional Marriage," "Democratic Voters," "Independent Voters," "Republican Voters," "Swing Dem Voters," and

---

[105] *The technology platform where data and advertising converge*, RETARGETLY, https://retargetly.com/ [https://perma.cc/LW77-KZ2M].

[106] *Holiday Campaign Planner: 3 Critical Strategies to (Re)Connect to Retail Mobile Customers*, TRUEDATA (Nov. 12, 2018), https://www.truedata.co/holiday-campaign-planner-3-critical-strategies-to-reconnect-to-retail-mobile-customers/ [https://perma.cc/8ALU-6DHZ].

[107] *Geo-Interest Expansion for CTV*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/api/doc/GeoInterestExpansion [https://perma.cc/G5LE-ZPVR].

[108] *comScore and i360 Team Up to Provide Digital Marketing Insights for Political Campaigns and Advocacy Groups*, PR NEWSWIRE (Apr. 17, 2012), https://www.prnewswire.com/news-releases/comscore-and-i360-team-up-to-provide-digital-marketing-insights-for-political-campaigns-and-advocacy-groups-147750205.html [https://perma.cc/4F88-VHPT]; *Data Quality*, I-360, https://www.i-360.com/why-i360/data-quality/ [https://perma.cc/5ZDK-4H7S].

[109] *Data Quality*, I-360, https://www.i-360.com/why-i360/data-quality/ [https://perma.cc/5ZDK-4H7S].

"Swing GOP Voters."[110] According to data partner Factual, "[w]ith Factual's datasets integrated into The Trade Desk platform, campaign managers can use hyperlocal segmentation to target mobile users" with a "level of precision" that "target[s] users in a specific area at the right time."[111] As noted above, Eyeota also offers extensive political segments for sale.

d. **Medical:** OnAudience, a data Partner that profiles Internet users by "observing user activity based on websites visited, content consumed and history paths to find clear behavior patterns and proper level of intent," lets customers target individuals categorized as interested in "Brain Tumor," "AIDS & HIV," "Substance Abuse," "Chronic Pain," and "Incest & Abuse Support."[112] Another Trade Desk data Partner, Medicx Health, rebranded OptimizeRx after a merger, offers a product called Micro-Neighborhood Targeting, a patient targeting product that "combines clinical eligibility, social determinants of health, media consumption, and geo-location to find and reach qualified patients on a diverse set of media and programmatic channels."[113]

e. **"Retail Media:"** Trade Desk partners with the grocery store giant, Albertsons "Media Collective," a "leader[] in one of the fastest-growing sectors in the online surveillance economy—called "retail media."[114] In a 2022 video, Trade Desk CEO Jeff Green describes the "missing piece" in advertising as "retailers making their data available so that advertisers can connect the dots from the very first activity and all of the subsequent touches all the way down to an individual purchase."[115] Through its relationship with Trade Desk, Albertsons is

---

[110] *Data Dictionary, Online Segments*, i-360, https://perma.cc/392Q-3RFL.

[111] *Making History: Programmatic in Politics*, THE TRADE DESK, at 14, https://democraticmedia.org/assets/resources/the_trade_desk_election2016_mar163.pdf [https://perma.cc/WA6L-397D].

[112] Dr. Johnny Ryan, *Submission to the Irish Data Protection Commission*, IRISH COUNCIL FOR CIVIL LIBERTIES (Sept. 21, 2020), https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf [https://perma.cc/Y2J6-Z9YF].

[113] OPTIMIZERRX, https://web.archive.org/web/20250216103743/https:/www.optimizerx.com/ [https://perma.cc/DM96-HBB3]; *Micro-Neighborhood Targeting*, OPTIMIZERX, https://www.optimizerx.com/micro-neighborhood-targeting [https://perma.cc/5KMS-WSE8].

[114] Jeff Chester, *The Commercial Surveillance Marketing Storm Driving the Albertsons and Kroger Deal*, TECHPOLICY.PRESS (Dec. 13, 2023), https://www.techpolicy.press/the-commercial-surveillance-marketing-storm-driving-the-albertsons-and-kroger-deal/ [https://perma.cc/SZ44-PHEZ].

[115] *The Trade Desk, In Human Terms, Episode 19: Retail Closes the Loop*, YOUTUBE (Jan. 18, 2022) https://www.youtube.com/watch?v=y83-Z1j4Ybc [https://perma.cc/GG3P-TQGC].

"connected to a vast network of data brokers that provide ready access to customer health, financial, and geolocation information."[116] As one privacy advocate explains: "[t]hey know precisely *what* you bought, browsed, and viewed—in store and at home."[117] The scale of a single retailer's ability to sell data about people on Trade Desk's Marketplace is staggering. Albertsons' Kristi Argyilan explained in discussion with Trade Desk's Chief Strategy Officer Samantha Jacobson: "We see over half of the US adult consumer population go through our doors, we see them about two and a half times a week. So we have an enormous amount of data points on customer behaviors and what large audiences of people are actually doing and buying and even how their lives are changing based on what their shopping patterns are."[118]

139. Trade Desk clients include not only businesses looking to advertise their wares, but also political campaigns seeking to surveil, investigate, or target particular individuals with propaganda. Indeed, Trade Desk markets directly to political parties.[119] In a 2020 interview, CEO Jeff Green said the company was helping "nearly all" 10 presidential candidates for the 2020 presidential election, as well as local campaigns. He explained that political advertising was a key revenue driver; Trade Desk was "feeling really great about the year . . . and that's largely driven by political advertising."[120]

140. Ahead of the 2024 presidential election, Trade Desk's focus on the connected TV ("CTV") market made it particularly well positioned to profit from political advertising and propaganda, as political campaigns significantly increased CTV ad spending.[121] Trade Desk

---

[116] Jeff Chester, *The Commercial Surveillance Marketing Storm Driving the Albertsons and Kroger Deal*, TECHPOLICY.PRESS (Dec. 13, 2023), https://www.techpolicy.press/the-commercial-surveillance-marketing-storm-driving-the-albertsons-and-kroger-deal/ [https://perma.cc/SZ44-PHEZ].

[117] *Id*.

[118] *Kokai Fireside chat featuring Albertson Media Collective's Kristi Argyilan*, YOUTUBE (June 26, 2023) https://www.youtube.com/watch?v=9ffdXW5BVBI [https://perma.cc/CMH9-Q4BX].

[119] *Supercharge your political advertising*, THE TRADE DESK, [https://perma.cc/6ZHF-2CMF].

[120] Tyler Clifford, *Trade Desk is behind seemingly ubiquitous 2020 online political ads, CEO says*, CNBC (Feb. 27, 2020), https://www.cnbc.com/2020/02/27/trade-desk-ceo-2020-election-ads-are-driving-our-business-this-year.html [https://perma.cc/N9YH-U6U5].

[121] Howard Homonoff, *2024 Political TV Advertising: We're Ready to Project the Winners*, FORBES (Nov. 30, 2023), https://www.forbes.com/sites/howardhomonoff/2023/11/30/2024-political-tv-advertising-were-ready-to-project-the-winners/ [https://perma.cc/RH8E-DDRR].

partners with third-party advertisers that specialize in political campaigns like Push Digital, GMMB, and ComScore to offer "new audience segments for political advertisers to help campaigns reach viewers across CTV platforms."[122]

141. Political campaigns now have "needle-in-the-haystack capabilities" to "microtarget voters on all their devices" using personal information sold by data brokers.[123] Trade Desk touts its ability to manipulate voters through their biases by sending "highly targeted campaign messages," explaining that "[e]ach voter is a unique person with a distinct set of interests, biases and viewpoints. The volume of data we aggregate in the marketplace gives political ad buyers the ability to inform every ad with knowledge of the user, and the ability to cater each message to the voter's interests. The result is a messaging platform that speaks the voter's language and speaks to their biases."[124]

142. Trade Desk enables any political campaign to "deliver a near one-to-one message to identified supporters as well as to target content or behaviors that are indicative of voter intent."[125] Combined with the massive digital dossiers in Trade Desk's systems, Trade Desk possesses the tools to enable direct manipulation of U.S. citizens, seamlessly targeting people everywhere they might seek information—their phones, computers, and TVs.

---

[122] Marty Swant, *Ad-tech firms and political agencies prepare for another year of spending heavily on CTV*, DIGIDAY (Oct. 27, 2023), https://digiday.com/media-buying/ad-tech-firms-and-political-agencies-prepare-for-another-year-of-spending-heavily-on-ctv/ [https://perma.cc/FB25-MY2J].

[123] Jeff Chester, *Our Next President: Also Brought to You by Big Data and Digital Advertising*, Bill Moyers (Jan. 6, 2017), https://billmoyers.com/story/our-next-president-also-brought-to-you-by-big-data-and-digital-advertising/ [https://perma.cc/R8FE-9J9W].

[124] *Making History: Programmatic in Politics*, THE TRADE DESK, at 12, https://democraticmedia.org/assets/resources/the_trade_desk_election2016_mar163.pdf [https://perma.cc/WA6L-397D]. ("Derive additional insights from your campaign by connecting existing campaign data around the users who already see your ads to third party data providers. For example, we found out that Democrats are more likely to buy grapefruit juice than Republicans. Democrats favor Tropicana, Snapple and Welch's. Republicans prefer Fuze, Sobe and Sunny D. By using these real-world insights, based purely on your campaign results, you uncover pockets of performance that no other media platform can provide.").

[125] *Programmatic advertising for political campaigns*, THE TRADE DESK (Dec. 11, 2023), https://www.thetradedesk.com/us/resource-desk/omnichannel-a-big-win-for-political-advertisers [https://perma.cc/68J6-QMVK].

143. The general public does not have access to Trade Desk's data marketplace, or visibility into who is buying and selling their information. Access is restricted to buyers and sellers, so individuals whose data is being bought and sold have no reasonable insight into what occurs there or the extent of Trade Desk's violations of their privacy rights.

144. Trade Desk does not publicly disclose the identity of its advertising clients that participate in its data marketplace. Plaintiffs and Class members have no reasonable basis to discern the identity of the persons and/or entities that buy or sell information about them on the Trade Desk data marketplace.[126] This opacity extends to possible state actors.

145. Trade Desk understands that its conduct as alleged herein is fundamentally privacy-violative; in a 2019 video describing privacy lines that should not be crossed "inside the confines of the quid pro quo of the internet," Trade Desk's CEO Jeff Green stated that "we have to find a way to respect privacy by not transacting in directly identifiable information or that really sensitive private information that you might share with a social network or with a search engine."[127] Yet, five years later—as explained in detail above—transacting in directly identifiable, sensitive, and private information *is at the heart of* Trade Desk's practices.

F. Trade Desk's Practices are Recognized as Highly Offensive and Invasive Threats to Individual Privacy

146. Trade Desk promotes UID2 as "privacy-conscious"[128] because it does not rely on third-party cookies to track individual users across the Internet and their devices. But industry leaders and commentators argue that the "cookieless" future is even bleaker from a privacy perspective than the adtech industry's past. "From a purely technical standpoint, [UID2 is] a regression in privacy in that [it] allow[s] tracking of users who are presently protected against tracking."[129]

---

[126] Nor, for that matter, does Trade Desk disclose what process it uses to vet data marketplace participants.

[127] The Trade Desk, *In Human Terms, Episode 7: Privacy*, YouTube (Dec. 4, 2019), https://www.youtube.com/watch?v=TTG5U5uSor0 [https://perma.cc/LE2D-CQB4].

[128] UNIFIEDID, https://unifiedid.com/ [https://perma.cc/8B86-BK45].

[129] Martin Thomson et al., *Comments on SWAN and Unified ID 2.0*, Mozilla (Aug. 4, 2021), https://blog.mozilla.org/en/mozilla/swan-uid2-privacy/ [https://perma.cc/AL8L-Q9R6].

147. "Cookieless" technologies like Trade Desk's generally depend on data provided by consumers ("first-party data") such as email addresses and phone numbers.[130] Identifiers that rely on first-party data, like UID2, "are more privacy-invasive than even cookies, and provide users with less transparency and control."[131] These identifiers "create persistent, identifiable connections to people across activity on multiple devices," and, according to a privacy advocate, are "even more robust of an identifier than your actual name or other [personally-identifiable information]."[132]

148. Privacy advocates at the Center for Digital Democracy have identified Trade Desk as playing an "outsized role" in the evolution away from cookies.[133] Despite positioning itself as essential to preserving the "open" Internet, Trade Desk's focus on serving the needs of advertisers has "reworked [the Internet] architecture to ensure we are all commercially surveilled," and "has continually expanded ways to monetize our behaviors, emotions, location and much more."[134]

149. Academic researchers have also raised the alarm about the false promises of "cookieless" advertising. The persistence of cookieless trackers like UID2 "can last for a greater duration than third-party cookies."[135] Identity resolution services like Trade Desk's "allow[] advertisers to develop rich profiles of existing customers through pairing data purchased from data brokers but also non-customers across the open web."[136] And cookieless trackers "encourage circumvention of targeting restrictions by advertising platforms" because there is "no mechanism

---

[130] Kate Kaye, *After Winning The Battle Over Third-Party Cookie Tracking, Will Privacy Advocates Lose The Personal-Data Use War?*, DIGIDAY (Mar. 29, 2021), https://digiday.com/media/after-winning-the-battle-over-third-party-cookie-tracking-will-privacy-advocates-lose-the-personal-data-use-war [https://perma.cc/2NHE-HV93].

[131] *Id.*

[132] *Id.*

[133] Jeff Chester, *Surveillance Marketing Industry Claims Future of an "Open Internet" Requires Massive Data Gathering*, CENTER FOR DIGITAL DEMOCRACY (July 31, 2021), https://democraticmedia.org/publishings/surveillance-marketing-industry-claims-future-open-internet-requires-massive-data-gathering [https://perma.cc/QY6W-58DL].

[134] *Id.*

[135] Ido Sivan-Sevilla and Patrick T. Parham, *Toward (Greater) Consumer Surveillance in a 'Cookie-less' World: A Comparative Analysis of Current and Future Web Tracking Mechanisms*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/system/files/ftc_gov/pdf/PrivacyCon-2022-Parham-Toward-Greater-Consumer-Surveillance-in-a-Cookie-less-World.pdf [https://perma.cc/FG6U-NEGM].

[136] *Id.*

to verify how advertisers have segmented first-party data before importing into these systems."[137] In short, "implementation of cookie-less tracking solutions by the AdTech complex potentially enables greater dynamic visibility on consumers, longer consumer tracking, and the assembling of more sensitive consumer profiles."[138] Far from the solution to the adtech industry's privacy problems, UID2 represents the most recent and most sophisticated *evolution* of them.

150. Privacy advocates have also focused on the interoperability of cookieless trackers like UID2 with CTV as a major source of privacy-invasive conduct.[139] "Connected television has become an essential link in the expanding data collection, identity tracking and targeting industry, enabling the capture of [first party data] . . . the most valuable kind of data sought by marketers."[140] A number of leading companies already use UID2, including "Fox's Tubi, Disney, Comcast, and Warner Bros. Discovery, Acxiom, Nielsen, Comscore and Experian."[141] Thus, "CTV enables advertising to become omnipresent, targeting highly personalized pitches designed to influence viewers everywhere"—including in their bedrooms, where they watch CTV, and where they do not expect their identities and activities to be collected and aggregated for the purpose of manipulating them through highly targeted advertising.[142]

151. Trade Desk has deliberately designed its technologies, including UID2, to be integrated and interoperable with those of other serial privacy violators. According to one privacy advocate, these "far-reaching partnerships among data brokers, publishers, adtech specialists, advertisers and marketing agencies" are united in service of the "key goal" of "establish[ing] a universal identifier for each of us, to directly capture our attention, reap our data, and monetize our behavior."[143]

---

[137] *Id.*

[138] *Id.*

[139] Jeff Chester and Kathryn C. Montgomery, *How TV Watches Us: Commercial Surveillance in the Streaming Era*, CENTER FOR DIGITAL DEMOCRACY (Oct. 2024), https://democraticmedia.org/assets/cdd-ctv-report-oct24-1.1.pdf [https://perma.cc/UY7K-YFEL].

[140] *Id.*

[141] *Id.* at 9.

[142] *Id.* at 4.

[143] Jeff Chester, *Surveillance Marketing 2.0*, CENTER FOR DIGITAL DEMOCRACY (June 30, 2022) https://democraticmedia.org/publishings/surveillance-marketing-2-0 [https://perma.cc/9D6F-

152. That Trade Desk's UID2 can circumvent existing privacy-preserving mechanisms likewise confirms the invasive nature of its technology.[144] For instance, Apple's "Do Not Track" feature, which prevents companies from collecting advertising identifiers, was specifically designed to prevent the type of user-specific tracking Trade Desk engages in. The creation of privacy-preserving browsers, which prevent the collection of third-party cookies, are likewise designed to prevent the type of online tracking conducted by Trade Desk.

G. Individuals Have Not Consented to Trade Desk's Tracking, Collection, or Use of Their Personal Information.

153. The long-established common law, statutory, and Constitutional rights to privacy are inherently and inextricably linked to fundamental cultural values of autonomy and freedom. The concept of "consent" reinforces these cultural values by functioning as a way for individuals to protect their privacy by exercising control over their personal information—what personal information organizations can collect, how they can use it, and to whom they can disclose it. Trade Desk conducts the business practices alleged in this complaint within a context and in a manner such that consent from the people whose data it assembles is not reasonably possible or practical. In fact, no such consent occurs. And in light of the extent of the privacy rights that are violated by Trade Desk's business practices, no consent to such practices could be enforced as a matter of law.

154. Plaintiffs and Class members, like our society at large, have no practical choice but to conduct their daily lives substantially in the digital world, connected to the Internet, with their personal information traveling through cyberspace every day. Much of daily life is now conducted online, including financial, commercial, or social activity. As a result, a person's Internet activity has become an "exhaustive chronicle" of their life. The personal information necessary for these activities courses through the Internet as these activities take place. When aggregated, this data can provide deep insight into a person's thinking, acting, and being. Without an expectation of privacy on the Internet, there would functionally be no expectation of privacy anywhere.

6JAU].

[144] Martin Thomson et al., *Comments on SWAN and Unified ID 2.0*, Mozilla (Aug. 4, 2021), https://blog.mozilla.org/en/mozilla/swan-uid2-privacy/ [https://perma.cc/AL8L-Q9R6].

155. Trade Desk sits atop a complex data collection and processing apparatus that feeds its labyrinthine multinational data marketplace. It is impossible for ordinary people to reasonably understand the true purpose and extent of Trade Desk's data collection, compiling of digital dossiers, and other data exploitation practices, which are opaque, if not invisible, to ordinary data subjects. Given the complexity and disguised nature of Trade Desk's collection and use of personal information, and the lack of any direct relationship between Trade Desk and the Plaintiffs and Class members, there is no reasonable basis for Plaintiffs and the Class members to know the extent to which Trade Desk is obtaining their data, tracking them, and selling their data or services derived from their data.

156. Trade Desk's presence on the Internet and in the digital world is ubiquitous, by design. Its data gathering activities are constant, vast, and encompass a massive swath of Internet activity. The breadth and complexity of sources from which Trade Desk compiles digital dossiers, or profiles, on Class members, including from credit card transactions[145] and interactions with brick-and-mortar establishments,[146] is such that as a practical matter, Plaintiffs and Class members have no way of knowing—and thus no way of even being able to consent to—the actual scope of Trade Desk's conduct. Plaintiffs and Class members, do not, merely by virtue of conducting the necessary activities of daily life, both online and in the physical world, consent to constant and pervasive surveillance by Trade Desk and the creation of detailed dossiers about them.

157. In as much as the Internet and digital existence has become integral to people's lives, its functioning and complexity with respect to personal information remain opaque to reasonably informed people. The Findings and Declarations of the California Privacy Rights Act (CPRA) notes

---

[145] Visa and Mastercard are both "partners" that provide Class members' data to Trade Desk for use in Trade Desk's products and services, as described herein. *Our Partners*, THE TRADE DESK, https://www.thetradedesk.com/us/our-platform/our-partners/partner-directory [https://perma.cc/5437-L7MH].

[146] *The Trade Desk Wants to Control Retail Media*, ADMONSTERS (May 8, 2023), https://www.admonsters.com/eletters/the-trade-seeks-control-retail-media/ [https://perma.cc/HD49-B7X9] (Trade Desk works "with retailers like Walmart, Target, and Home Depot to help advertisers buy programmatic ads powered by retailers' data."; According to CEO Jeff Green, "Now you can show an ad to a consumer and then see when that same consumer actually buys it in a brick-and-mortar store—it creates a level of efficiency in the open internet that we've never had before"); *Trade Desk's Jeff Green Talks Retail Media: Investor Day*, BUSINESS INSIDER (Oct. 4, 2022), https://www.businessinsider.com/the-trade-desks-jeff-green-talks-retail-media-investor-day-2022-10 [https://perma.cc/3VCW-6ASX].

that the "asymmetry of information" inherent in the "collect[ion] and use [of] consumers' personal information . . . makes it difficult for consumers to understand what they are exchanging and therefore to negotiate effectively with businesses." There is asymmetry of knowledge between Trade Desk and the data subjects it exploits, including Plaintiffs and Class members, in that Trade Desk has complete knowledge of its data collection and data exploitation practices, but Plaintiffs and Class members have no direct relationship with Trade Desk regarding these practices and no reasonable basis to discern those practices nor the nature of the practices directed at them.

158. Plaintiffs and Class members cannot reasonably foresee all the ways in which Trade Desk may use the detailed dossiers it is compiling on them. Plaintiffs and Class members have no way of knowing the specific third parties to which Trade Desk will provide their personal information, or what those third parties will do with that information. Plaintiffs and Class members thus cannot provide knowing and informed consent to Trade Desk's dissemination of their personal information.

159. Trade Desk makes no pretense of having directly obtained consent from the people whose data it gathers, including Plaintiffs and Class members. At no point during its process of collecting or processing personal information, or the compiling of dossiers or selling services based on that personal information, does Trade Desk ever directly ask individuals for their consent. Despite the fact that Trade Desk "does not have a direct relationship" with the subjects whose data it exploits, Trade Desk has failed to register as a data broker with the State of California,[147] thereby further obscuring and hiding the true nature of its business activities from Plaintiffs and Class members. *See* Cal. Civ. Code § 1798.99.80.

160. Nor have Plaintiffs and Class members manifested any form of consent indirectly to Trade Desk. Trade Desk publishes so-called privacy policies on its website, but these policies are not reasonably directed to Plaintiffs and Class members, all of whom lack any direct relationship with Trade Desk and have no reasonable insight into Trade Desk's data collection and data exploitation practices or how they may or may not be subject to such practices. Therefore, there is

[147] *See* California Privacy Protection Agency 2025 Data Broker Registry List, available at https://cppa.ca.gov/data_broker_registry/registry.csv.

no reasonable basis for Plaintiffs and Class members to be aware of Trade Desk's privacy policies or to have directed themselves to them. Plaintiffs and Class members are not legally subject to or governed by Trade Desk's published privacy policies.

161. Trade Desk's so-called privacy policies are themselves insufficient to adequately inform Plaintiffs and Class members about the nature and extent of Trade Desk's data collection and data exploitation practices, even with regard to their personal information. Plaintiffs and Class members are in the course of daily life barraged with thousands of pages of purported "terms and conditions" and "privacy policies" for online products and services. Computer science researchers have estimated that, based on the number of unique sites American Internet users visit annually, it would take the average Internet user between 181 to 304 hours to read the relevant privacy policies. This translates to approximately 72 billion hours per year for every U.S. Internet user to read all the privacy policies that they encounter. Trade Desk knows, or reasonably should know, that it is not reasonably possible for Internet users to read or comprehend the thousands of privacy policies they encounter, including Trade Desk's privacy policies.

162. As privacy scholars have noted, issues that users must navigate to understand the significance of consent are too complex and the conditions surrounding consent too easy to manipulate for any purported consent to be informed and meaningful. It is well-known that many websites include "cookie popups" that purport to ask for consent for the website placing a cookie on the users' computer. In practice, however, most formulations of user control rights fail to sufficiently explain that cookie tracking leads to profiling based on information derived from user behavior. These practices, whether by Trade Desk or other third parties, fail to provide sufficient means to obtain the legally viable consent to Trade Desk's mass data collection, behavior tracking, and assembling of dossiers based on that data.

163. In practice, the "notice and consent" framework that permeates the Internet is farcical. For example, a recent forensic investigation revealed that, in the context of the IAB[148]

[148] The "Interactive Advertising Bureau (IAB) is an American advertising business organization that develops industry standards, conducts research, and provides legal support for the online advertising industry." Wikipedia, *Interactive Advertising Bureau*, https://en.wikipedia.org/wiki/Interactive_Advertising_Bureau [https://perma.cc/FP9B-VE7B].

Europe's "Transparency Consent Framework" (TCF), even when users specifically decline consent to be tracked, various adtech participants—including Trade Desk —ignore those declinations and place trackers on users' devices.[149] The study discovered that Trade Desk places tracking cookies on a user's device *before the user even has a chance to decline consent.*[150] In fact, even before the user has a chance to consent, a pixel sent from Trade Desk encodes the user's "geo-location, including his longitude, latitude, and even the temperature outside his office at the time."[151]

164. As the study understatedly mused in observing Trade Desk's utter disregard of the user's explicit privacy preferences: "It is not clear why The Trade Desk's servers in Washington, when notified by the TCF string that the user specifically has neither provided consent for cookies or for personalized profiling, are still setting persistent cookies in [the user's] browser. It is also not clear why [data broker] Experian and The Trade Desk's servers are exchanging unique user data about Charlotte, when both parties have received a TCF string that specifically dis-allows such behavior."[152] The IAB's CCPA Framework is broadly similar to the European TCF, and is directed at Internet users in California.[153]

---

[149] *Are Ad Tech Vendors in Europe Ignoring User Consent Signals?*, ADALYTICS, https://adalytics.io/blog/adtech-not-checking-user-tcf-consent [https://perma.cc/W2R6-SUMY] ("Pierre's TCF string shows that he only consented to basic ads (and only from Google). He is curious as to whether this ad creative that was served to his browser is indeed a "basic ad", devoid of any tracking or measurement pixels. He takes a look at the details of the "ad" attribute that was sent in the HTTPS response. The Balenciaga ad contains tracking and ad viewability or render pixels from TripleLift, Google, Oracle Moat, and The Trade Desk.").

[150] *Id.* ("An EU citizen with a German IP address installs Google Chrome on their desktop for the first time. This new instance of Chrome is not logged into any accounts or emails, and has no cookies or local storage. The user visits a wsj.com article, and is shown a consent banner . . . *Before this user has an opportunity to click on any specific consent icons or buttons, the user's browser makes dozens of HTTP requests to third party domains*, belonging to companies such as Google, Adobe, New Relic, Cxense, and The Trade Desk. Many of these HTTP requests contain response headers that set tracking cookies in the user's browser. For example, an HTTP request made to match.adsrvr.org sets a cookie in the user's browser called "TDID"; this cookie is set to expire in 365 days. The Trade Desk's documentation explains that this is a unique identifier generated for a given user, and is designed to allow syncing user data with other ad tech companies.") (emphasis added).

[151] *Id.*

[152] *Id.*

[153] James Hercher, *The IAB Finalizes CCPA Framework As Industry Readies For More Regulators*, AD EXCHANGER (Dec. 5, 2019), https://www.adexchanger.com/online-advertising/the-iab-finalizes-ccpa-framework-as-industry-readies-for-more-regulators/ [https://perma.cc/Q2CX-GLU4].

165. Neither Trade Desk's so-called privacy policies nor the policies of third-party Internet publishers could provide any reasonable basis for Plaintiffs and Class members to have consented to Trade Desk's data collection, compiling of digital dossiers, and other data exploitation practices, or to have waived their privacy rights, including to be free from Trade Desk's pervasive surveillance of them.

166. Trade Desk knows, or reasonably should know, that Internet users such as Plaintiffs and Class members have insufficient knowledge or basis to reasonably comprehend the extent to which Trade Desk is obtaining their data, tracking their activity, and compiling it into digital dossiers, nor the deeply invasive and detailed nature of those dossiers. Trade Desk makes no disclosure anywhere directly to Plaintiffs or Class members of these practices. To the extent that Plaintiffs or Class members indirectly acknowledge to third parties the presence of some aspect of an isolated data collection practice, or tracking cookie on an individual website, such acknowledgement in no way does or could reflect any consent or sufficient understanding of Trade Desk's practices.

167. Trade Desk effectuates ongoing, comprehensive surveillance of Plaintiffs and Class members which grievously intrudes upon their privacy and which inevitably results in the corrosion of their individual autonomy and the collective autonomy of society at large. Ordinary people, such as Class members, do not and cannot possess an appropriate level of knowledge about the substantial threats that Trade Desk's surveillance poses to their own autonomy (in addition to lacking information sufficient to comprehend the nature and extent of Trade Desk's surveillance and its other implications). The social harms posed by Trade Desk's conduct impair not only individual autonomy, but the collective autonomy of Class members. This is because all members of a society have an interest in the enforcement of privacy rights, freedom from surveillance, and preservation of autonomy. Evisceration of these privacy values inexorably leads to the abrogation of peoples' autonomy and freedom, which are essential to the proper functioning of democratic republics. These harms caused by Trade Desk far outweigh the commercial benefits that extend to a private corporation. In the context of Trade Desk's practices, valid consent from Plaintiffs and Class members is not only absent, it is not even possible.

168. Trade Desk is well aware that consumers do not and cannot consent to its acquisition and use of their data. In advertisements urging adoption of its UID2 identifier, Jeff Green, Founder and CEO of Trade Desk, candidly acknowledged that "of course, as consumers, we're never going to read" the privacy policies on individual websites that purport to provide consent to third parties' provision of Class members' personal information to Trade Desk.[154]

169. Plaintiffs and Class members have not waived their fundamental right to be free from the pervasive surveillance to which Trade Desk subjects them. In any event, even were there any basis to conclude that Plaintiffs and Class members could be considered to have waived their reasonable expectation of privacy with respect to Trade Desk's practices (and there is not), such waiver would be void and invalid as against public policy.

VIII. CLASS ALLEGATIONS

170. Plaintiffs bring this class action, pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes, which is referred to throughout this Complaint as the "Classes:"

> **United States Class for Intrusion Upon Seclusion, Unjust Enrichment, and Declaratory Relief ("United States Class"):**
>
> All natural persons located in the United States whose personal information, or data derived from their personal information, was made available for sale or use through Trade Desk.
>
> **United States Sub-Class for Violations of the Electronic Communications Privacy Act ("ECPA"), the California Invasion of Privacy Act ("CIPA"), and the California Comprehensive Computer Data Access and Fraud Act ("CDAFA") Sub-Class ("Statutory Sub-Class"):**
>
> All members of the United States Class whose contents of their electronic communications were intercepted by Trade Desk, or whose routing, addressing or signaling information was recorded by Trade Desk, or on whose devices Trade Desk's UID2 token, Universal Pixel, Static Tracking Pixel, Real Time Conversion Events SDK, TDID, or other Trade Desk cookies were deposited and transmitted data to Trade Desk.
>
> **California Sub-Class for Violation of Privacy under the California Constitution ("California Sub-Class"):**

[154] The Trade Desk, *In Human Terms, Episode 15: Unified ID 2.0*, YOUTUBE at 3:17 (Nov. 18, 2020), https://www.youtube.com/watch?v=mJP2ngh0owc [https://perma.cc/7KGQ-GDWF].

> All members of the United States Class located in California whose personal information, or data derived from their personal information, was made available for sale or use through Trade Desk.

171. Excluded from the Classes are the following individuals: officers and directors of Trade Desk and its parents, subsidiaries, affiliates, and any entity in which Trade Desk has a controlling interest, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

172. Plaintiffs reserve the right to modify or amend the definition of each of the proposed Classes before the Court determines whether certification is appropriate.

173. This action readily satisfies the requirements set forth under Federal Rule of Civil Procedure 23.

174. **Numerosity:** Each Class is so numerous that joinder of all members is impracticable. Upon information and belief, Class members number in the millions.

175. **Commonality:** There are questions of law or fact common to the Classes. These questions include, but are not limited to, the following:

a. Whether Trade Desk's acts and practices complained of herein amount to egregious breaches of social norms;

b. Whether Trade Desk acted intentionally in violating Plaintiffs' and Class Members' privacy rights;

c. Whether at-issue communications qualify as "electronic communications"

d. Whether Trade Desk intercepted communications "content;"

e. Whether Trade Desk was unjustly enriched as a result of its violations of Plaintiffs' and Class Members' privacy rights;

f. Whether an injunction should issue; and

g. Whether declaratory relief should be granted.

176. **Typicality:** Plaintiffs' claims are typical of the claims of the Classes. Plaintiffs and the Class Members did not consent to Trade Desk's interception, collection, analysis, and sale or their personal information, which acts form the basis for this suit.

177. Moreover, like all Class Members, Plaintiffs suffer a substantial risk of repeated injury in the future. Plaintiffs continue to use devices that are capable of reporting personal information to Trade Desk. Trade Desk's actions have thwarted and continue to threaten Plaintiffs' and Class Members' ability to exercise control over their own privacy while using their devices. Because the conduct complained of herein is systemic, Plaintiffs and all Class Members face substantial risk of the same injury in the future. Trade Desk's conduct is common to all Class Members and represents a common pattern of conduct resulting in injury to all Class Members. Plaintiffs have suffered the harm alleged and have no interests antagonistic to any other Class Member.

178. **Adequacy:** Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs' interests do not conflict with the interests of Class Members. Furthermore, Plaintiffs have retained competent counsel experienced in class action litigation, consumer protection litigation, and electronic privacy litigation. Plaintiffs' counsel will fairly and adequately protect and represent the interests of the Classes.

179. Trade Desk has acted on grounds generally applicable to the Classes, thereby making final injunctive relief and corresponding declaratory relief each appropriate with respect to the Classes as a whole. The prosecution of separate actions by individual Class Members would create the risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Trade Desk.

IX. CAUSES OF ACTION

First Cause of Action
Invasion of Privacy Under the California Constitution
(on behalf of the California Sub-Class)

180. Plaintiffs and the California Sub-Class members reallege and incorporate by reference each allegation in the preceding paragraphs contained herein.

181. Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property and pursuing and obtaining safety,

happiness, *and privacy*." The phrase "*and privacy*" was added by the "Privacy Initiative" adopted by California voters in 1972.

182. The addition of the phrase "and privacy" occurred after voters approved a proposed legislative constitutional amendment designated as Proposition 11. Proposition 11 was intended to curb businesses' control over the unauthorized collection and use of peoples' personal information, as the ballot argument stated:

> The right of privacy is the right to be left alone. . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom.[155]

183. This amended constitutional provision addresses the concern over accelerating encroachment on personal freedom and security caused by increasing surveillance and data collection activity in contemporary society. Its proponents meant to afford individuals more measures of protection against this most modern threat to personal privacy:

> Computerization of records makes it possible to create 'cradle-to-grave' profiles of every American. At present there are no effective restraints on the information activities of government and business. This amendment creates a legal and enforceable right of privacy for every Californian.[156]

In recognizing these privacy rights, the California Constitution provides insight into and serves to define the nature of the reasonable expectation of privacy of an objectively reasonable California resident. In contravention to the California Constitution and the reasonable expectations of privacy of California residents, Trade Desk "stockpil[es] unnecessary information about [Class members] and [] misus[es]information gathered for one purpose in order to serve other purposes," creating "cradle-to-grave" profiles of Class members.

184. Plaintiffs and the California Sub-Class members maintain a reasonable expectation of privacy in the conduct of their lives, including their Internet browsing activities, and in their

---

[155] Ballot Pamp., Proposed Stats. & Amends. To Cal. Const. With Arguments to Voters. Gen. Election *26 (Nov. 7, 1972).
[156] *Id.*

electronic communications and exchange of personal information. The reality of modern life increasingly requires that much of our daily activities are conducted online—Plaintiffs and the California Sub-Class members have no practical choice or ability but to conduct their daily lives substantially in the digital world, connected to the Internet. The necessary engagement with the digital world makes Plaintiffs' and the California Sub-Class members' private lives susceptible to unlawful observation and recording, capable of yielding a comprehensive and intrusive chronicle of Plaintiffs' and the California Sub-Class members' lives. If Plaintiffs and the California Sub-Class members cannot have a reasonable expectation of privacy in the conduct of their lives online and the digital transmission of their personal information, they can have no reasonable expectation of privacy for virtually any facet of their lives.

185. Trade Desk, in violation of Plaintiffs' and the California Sub-Class members' reasonable expectation of privacy, intercepts, collects, tracks, and compiles their Internet activity and communications, and makes available for sale access to that data as well.

186. The nature and volume of the data collected is such that Trade Desk's practice of compiling comprehensive identity profiles violates Plaintiffs' and the California Sub-Class members' reasonable expectation of privacy. Technological advances, such as Trade Desk's use of cookies, pixels, real-time bidding, and other means to track and compile Internet activity and electronic communications, provide Trade Desk with the means to assemble a comprehensive chronicle of Plaintiffs' and the California Sub-Class members' lives heretofore unseen. Trade Desk collects and compiles personal information such as Plaintiffs' and the California Sub-Class members' email addresses, location data, web browsing information, including that relating to race, religion, sexual orientation, and health. Such information is "personal information" under California law, which defines personal information as including "[i]nternet or other electronic network activity information," such as "browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement." Cal. Civ. Code § 1798.140.

187. Trade Desk also collects and analyzes Plaintiffs' and the California Sub-Class members' real-world offline activity and compiles computerized records of those activities.

Plaintiffs' and the California Sub-Class members do not and cannot know which specific real-world offline activities Trade Desk may or may not be collecting and analyzing and adding to the digital dossiers it compiles on them.

188. Trade Desk's conduct as described herein is highly offensive to a reasonable person and constitutes an egregious breach of social norms, specifically including the following:

a. Trade Desk engages in dragnet-style collection and interception of Plaintiffs' and the California Sub-Class members' Internet activity, including their communications with websites, without California Sub-Class members' knowledge or consent.

b. Trade Desk also collects details about Plaintiffs' and the California Sub-Class members' *offline* activities. By its very nature, Plaintiffs' and the California Sub-Class members cannot be aware of or consent to this conduct.

c. Trade Desk creates comprehensive identity profiles based on this online and offline data, which constitute precisely the sort of computerized "cradle-to-grave profiles" that the right to privacy under the California Constitution was created to constrain.

189. Trade Desk's amassing of electronic information reflecting highly detailed aspects of Plaintiffs' and the California Sub-Class members' lives into dossiers, both directly and through providing access to its data marketplace, for future or present use, is in and of itself a violation of Plaintiffs' and the California Sub-Class members' right to privacy in light of the serious risk these dossiers pose to their autonomy. Additionally, these dossiers are and can be used to further invade Plaintiffs' and the California Sub-Class members' privacy, by, inter alia, allowing third parties to learn intimate details of Plaintiffs' and the California Sub-Class members' lives, and target them for advertising, political, and other purposes, as described herein, thereby harming them through the abrogation of their autonomy and their ability to control dissemination and use of information about them. Additionally, as described above, the social harms posed by Trade Desk's conduct impair not only individual autonomy, but the collective autonomy of the California Sub-Class members, and autonomy is essential to the proper functioning of democratic republics.

190. Privacy advocates have repeatedly decried Trade Desk's practices as harmful and highly offensive.

191. Trade Desk has violated Plaintiffs' and the California Sub-Class members' reasonable expectation of privacy via Trade Desk's review, analysis, dissemination, and subsequent uses of Plaintiffs' and California Sub-Class members' Internet activity through Trade Desk's identity graph systems and data marketplace.

192. Trade Desk's practices as alleged herein violate Plaintiffs' and the California Sub-Class members' reasonable expectation of privacy, are highly offensive to a reasonable person, and constitute an egregious breach of social norms.

193. Trade Desk's violations of various state and federal statutes, and its actions to enable others to violate various state and federal statutes relating to privacy protections are each an independent and egregious breach of social norms.

194. The California Constitution created an inalienable right to be free from pervasive electronic surveillance; Plaintiffs and the California Sub-Class members are under no obligation to "opt out" of such violations of their constitutional privacy rights to stop Trade Desk's intrusions into their daily lives—that right inheres automatically for every California Sub-Class member.

195. The right to privacy in California's constitution creates a right of action for California residents against private entities such as Trade Desk. Trade Desk lacks a legitimate business interest in stockpiling and compiling the personal information of Plaintiffs and the California Sub-Class members.

196. Plaintiffs and the California Sub-Class members have been damaged by Trade Desk's invasion of their privacy and are entitled to just compensation and injunctive relief.

Second Cause of Action
Intrusion Upon Seclusion Under California Common Law
(on behalf of the United States Class)

197. Plaintiffs reallege and incorporate by reference each allegation in all preceding paragraphs contained herein.

198. California common law on intrusion upon seclusion is applicable for all members of the United States Class.

199. A plaintiff asserting a claim for intrusion upon seclusion must plead (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

200. Plaintiffs and United States Class members maintain a reasonable expectation of privacy in the conduct of their lives, including their Internet browsing activities and in their electronic communications and exchange of personal information. The reality of modern life increasingly requires that much of our daily activities are conducted online—Plaintiffs and United States Class members have no practical choice or ability but to conduct their daily lives substantially in the digital world, connected to the Internet. The necessary engagement with the digital world makes Plaintiffs' and United States Class members' private lives susceptible to unlawful observation and recording that is capable of yielding a comprehensive and intrusive chronicle of their lives. If Plaintiffs and United States Class members cannot have a reasonable expectation of privacy in the conduct of their lives online and the digital transmission of their personal information, they can have no reasonable expectation of privacy for virtually any facet of their lives.

201. Trade Desk, in violation of Plaintiffs' and United States Class members' reasonable expectation of privacy, intercepts, collects, tracks, and compiles their Internet activity and communications, and makes access to that data available for sale as well.

202. The nature and volume of the data collected is such that Trade Desk's practice of compiling comprehensive identity profiles violates Plaintiffs' and United States Class members' reasonable expectation of privacy. Technological advances, such as Trade Desk's use of cookies, pixels, real-time bidding, and other means to track and compile Internet activity and electronic communications, provide Trade Desk with the means to assemble a comprehensive chronicle of Plaintiffs' and United States Class members' lives heretofore unseen. Trade Desk collects and compiles personal information such as Plaintiffs' and United States Class members' email addresses, location data, and web browsing information, including information relating to race, religion, sexual orientation, and health. Such information is "personal information" under California law. Cal. Civ. Code § 1798.140 (defining personal information as including "Internet or other electronic network activity information," such as "browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.").

203. Trade Desk also collects and analyzes Plaintiffs' and United States Class members' real-world offline activity and compiles computerized records of those activities. Plaintiffs and United States Class members do not and cannot know which specific real-world offline activities Trade Desk may or may not be collecting and analyzing and adding to the digital dossiers it compiles on them.

204. Trade Desk's conduct as described herein is highly offensive to a reasonable person and constitutes an egregious breach of social norms, specifically including the following:

a. Trade Desk engages in dragnet-style collection and interception of Plaintiffs' and United States Class members' Internet activity, including their communications with websites, without United States Class members' knowledge or consent.

b. Trade Desk also collects details about Plaintiffs' and United States Class Members' *offline* activities. By its very nature, Plaintiffs and United States Class members cannot be aware of or consent to this conduct.

c. Trade Desk creates comprehensive profiles based on this online and offline data, which constitute precisely the sort of computerized "cradle-to-grave profiles" the right to privacy under the California Constitution was created to constrain.

d. Trade Desk violates federal and state statutes designed to protect United States Class Members' privacy, including but not limited to the causes of action alleged herein.

205. Trade Desk's amassing of electronic information reflecting highly detailed aspects of Plaintiffs' and United States Class Members' lives into dossiers, both directly and through providing access to its data marketplace, for future or present use, is in and of itself a violation of Plaintiffs' and United States Class members' right to privacy in light of the serious risk these dossiers pose to their autonomy. Additionally, these dossiers are and can be used to further invade Plaintiffs' and United States Class Members' privacy, by, inter alia, allowing third parties to learn intimate details of Plaintiffs' and United States Class Members' lives, and target them for advertising, political, and other purposes, as described herein, thereby harming them through the abrogation of their autonomy and their ability to control the dissemination and use of information about them. Additionally, as described above, the social harms posed by Trade Desk's conduct

impair not only individual autonomy, but the collective autonomy of United States Class members, and autonomy is essential to the proper functioning of democratic republics.

206. Privacy advocates have repeatedly decried Trade Desk's practices as harmful and highly offensive.

207. Trade Desk has violated Plaintiffs' and United States Class members' reasonable expectation of privacy via Trade Desk's review, analysis, dissemination, and subsequent uses of Plaintiffs' and United States Class members' Internet activity through Trade Desk's identity graph system and data marketplace.

208. Trade Desk's practices as alleged herein violate Plaintiffs' and United States Class members' reasonable expectation of privacy, are highly offensive to a reasonable person, and constitute an egregious breach of the social norms.

209. Trade Desk lacks a legitimate business interest in stockpiling and compiling the personal information of Plaintiffs and United States Class members.

210. Plaintiffs and United States Class members have been damaged by Trade Desk's invasion of their privacy and are entitled to just compensation and injunctive relief.

211. As a result of Trade Desk's actions, Plaintiffs and United States Class members seek injunctive relief in the form of Trade Desk's cessation of tracking practices in violation of Plaintiffs' and United States Class members' rights, and destruction of all personal information obtained in violation of Plaintiffs' and United States Class members' rights.

212. As a result of Trade Desk's actions, Plaintiffs and United States Class members seek nominal and punitive damages in an amount to be determined at trial. Plaintiffs and United States Class members seek punitive damages because Trade Desk's actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiffs and United States Class members and made in conscious disregard of their rights. Punitive damages are warranted to deter Trade Desk from engaging in future misconduct.

213. Plaintiffs and United States Class members seek restitution for the unjust enrichment obtained by Trade Desk as a result of unlawfully collecting Plaintiffs' and United States Class members' personal information. These intrusions are highly offensive to a reasonable person.

Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiffs' and United States Class members' personal information with potentially countless third parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Trade Desk's conduct is the fact that Trade Desk's principal goal is and was to surreptitiously monitor Plaintiffs and the United States Class members and to allow third parties to do the same.

214. The threat posed by advancements in technology and the ability to create detailed dossiers therefrom was recognized half a century ago by Professor Arthur R. Miller.[157] With monumental increases in technologies, Professor Miller's alarm 50 years ago about technology's assault on privacy has now taken on special urgency: the precise concerns he warned of have come to fruition in Trade Desk's conduct. Through this lawsuit, Plaintiffs and United States Class members seek to vindicate their common law right against Trade Desk's ongoing assault on their privacy.

Third Cause of Action
Violation of The Federal Wiretap Act, 18 U.S.C. § 2510, et. seq.
(on behalf of the Statutory Sub-Class)

215. Plaintiffs and the Statutory Sub-Class reallege and incorporate by reference each allegation in the preceding paragraphs contained herein.

216. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986 ("ECPA") prohibits the intentional interception of the contents of any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

217. The ECPA protects both the sending and receipt of communications.

218. The ECPA provides a private right of action to any person whose electronic communications are intercepted, disclosed, or intentionally used in violation of the ECPA. 18 U.S.C. § 2520(a).

219. Trade Desk intentionally intercepted electronic communications that Plaintiffs and Statutory Sub-Class members exchanged with websites by tracking individuals while they were

[157] *See generally* Arthur R. Miller, *The Assault on Privacy* 24–54 (1971).

browsing the Internet through the direct placement and utilization of its source code on websites and apps as described below.

220. Trade Desk's actions in intercepting and tracking user communications while they were browsing the Internet was intentional. On information and belief, Trade Desk is aware that it is intercepting communications in these circumstances and has taken no remedial action.

221. Trade Desk's interception of Internet communications that Plaintiffs and Statutory Sub-Class members were sending and receiving was done contemporaneously with the sending and receipt of those communications.

Interception Through Pixels

222. As described above at paragraphs 94–103, Trade Desk places its Universal Pixel and Static Tracking Pixel software on websites such that it captures and transmits information as an individual navigates through webpages on which it is present. These trackers intercept actions taken, product views, purchase intent, and other content communications taken on websites.

223. On information and belief, Trade Desk has used its pixel software to intercept the content of Plaintiffs' and Statutory Sub-Class members' communication, including but not limited to:

a. the precise URL being viewed by the user;

b. the referrer URL;

c. information regarding actions being taken by the user;

d. purchase content and pricing;

e. the contents of search queries; and

f. button clicks and other affirmative selections on websites.

224. Examples of websites where Trade Desk's pixels have intercepted the contents of Plaintiffs' communications with websites are listed at paragraphs 17, 30, 43, and 53 above.

225. The transmission of data between Plaintiffs and Statutory Sub-Class members on the one hand and the websites on which Trade Desk tracked and intercepted their communications on the other, without authorization were "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic,

photoelectronic, or photooptical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

226. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The computer codes and programs Trade Desk used to track Plaintiffs' and Statutory Sub-Class members' communications, including JavaScript code;

b. Plaintiffs' and Statutory Sub-Class members' browsers and mobile applications;

c. Plaintiffs' and Statutory Sub-Class members' computing and mobile devices;

d. The computer codes and programs used by Trade Desk to effectuate its tracking and interception of Plaintiffs' and Statutory Sub-Class members' communications; and

e. The plan Trade Desk carried out to effectuate its tracking and interception of Plaintiffs' and Statutory Sub-Class members' communications while browsing the Internet.

227. Trade Desk, in its conduct alleged here, was not providing an "electronic communication service," as that term is defined in 18 U.S.C. § 2510(12) and is used elsewhere in the Wiretap Act. Trade Desk was not acting as an Internet Service Provider (ISP).

228. Trade Desk was not an authorized party to the communication because Plaintiffs and Statutory Sub-Class members were unaware of Trade Desk's interception of their communications with websites, and did not knowingly send any communication to Trade Desk. Trade Desk could not manufacture its own status as a party to Plaintiffs' and Statutory Sub-Class members' communications with others by surreptitiously intercepting those communications.

229. As described above, the communications between Plaintiffs and Statutory Sub-Class members on the one hand, and websites on the other, were simultaneous to, but *separate* from, the channel through which Trade Desk acquired the contents of those communications.

Interception Through Real-Time Events Conversion

230. Trade Desk's "Real Time Conversion Events SDK" is a software development kit that captures and transmits information as an individual interacts with an application or website

where it is integrated.[158] The Real Time Conversion Events SDK is designed to gain insight and understanding into users' activities and interactions within an application or website, such as actions taken, product views, purchase intent, ad conversions (*e.g.*, when a user interacts with a specific ad), and other content communications within the application or website.

231. When a user interacts with an application or website where the Real Time Conversion Events SDK is integrated, Trade Desk receives, at minimum:[159]

a. The content of the user's communication, including: the precise URL or in-app screen being viewed by the user; the referrer URL or previous in-app screen; information regarding actions being taken by the user, such as add-to-cart or purchase events; purchase content and pricing; the contents of search queries.

b. The IP address of the user's device;

c. The precise date and time of the interaction;

d. Unique device identifiers (such as UID2, TDID, IDFA, AAID, NAID, and DAID);

e. "User-Agent" (information regarding the specific device being used); and

f. Information regarding the user's location.

232. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The source code Trade Desk uses to track Plaintiffs' and Statutory Sub-Class members' communications;

b. Plaintiffs' and Statutory Sub-Class members' browsers;

c. Plaintiffs' and Statutory Sub-Class members' computing and mobile devices; and,

d. The plan Trade Desk carried out to effectuate its tracking and interception of Plaintiffs' and Statutory Sub-Class members' communications while browsing the Internet.

---

[158] *Real-Time Conversion Events*, THE TRADE DESK PARTNER PORTAL, https://partner.thetradedesk.com/v3/portal/data/doc/DataConversionEventsApi [https://perma.cc/WY4N-6XZE].

[159] *Id*.

233. Trade Desk is not a party to Plaintiffs' and Statutory Sub-Class members' communications with the websites they visit.

234. Trade Desk receives the content of Plaintiffs' and Statutory Sub-Class members' communications through the surreptitious redirection of those communications from Plaintiffs' and Statutory Sub-Class members' computing devices.

235. Trade Desk's learning, or attempting to learn, the contents of Plaintiffs' and Statutory Sub-Class members' communications occurred while they were in transit or in the process of being sent or received.

Lack of Consent

236. Plaintiffs and Statutory Sub-Class members were unaware of, and did not consent to, Trade Desk's acquisition of their communications with the websites they visited, as described above. Trade Desk did not obtain legal authorization to obtain Plaintiffs' and Statutory Sub-Class members' communications with the websites they visited. Any purported consent that Trade Desk received from websites to obtain the content of Plaintiffs' and Statutory Sub-Class members' communications was not valid.

237. The scope, ubiquity, and unavoidability of Trade Desk's interceptions defeat any affirmative consent that Trade Desk may raise regarding consent in that Trade Desk has not obtained consent from anyone to intercept communications content on thousands of websites and apps using a process including UID2 to identify the Statutory Sub-Class members who made those communications for purposes of creating highly detailed dossiers on Statutory Sub-Class members.

The Interceptions Were Performed for the Purpose of Committing Tortious Acts

238. In acquiring the content of Plaintiffs' and Statutory Sub-Class members' communications with websites, Trade Desk had a purpose that was tortious and designed to violate state constitutional and common law. Consent is not a defense where a "communication is intercepted for the purpose of committing any criminal or tortious act." 18 U.S.C. § 2511(2)(d). Subsequent use or disclosure of the contents of the intercepted communications for the purpose of further invading Plaintiffs' and Statutory Sub-Class members' privacy is a tortious act that satisfies this exception to consent. In addition to having the intent of profiting from the sale of Plaintiffs'

and Statutory Sub-Class members' personal information, Trade Desk knowingly and intentionally invaded Plaintiffs' privacy through intercepting their communications and using the fruits of those interceptions to further invade Plaintiffs' and Statutory Sub-Class members' privacy through the creation of cradle-to-grave dossiers on them and the facilitation of the purchase and sale of their detailed personal information.

239. For Trade Desk's violations set forth above, Plaintiffs and Statutory Sub-Class members seek appropriate equitable or declaratory relief, including injunctive relief; actual damages and "any profits made by [Trade Desk] as a result" of its violations or the appropriate statutory measure of damages; punitive damages in an amount to be determined by a jury; and reasonable attorney's fee and other litigation costs reasonably incurred pursuant to 18 U.S.C § 2520.

240. Unless enjoined, Trade Desk will continue to commit the violations of law alleged here.

241. Pursuant to 18 U.S.C. § 2520, Plaintiffs and Statutory Sub-Class members seek monetary damages for the greater of (i) the sum of the actual damages suffered by Plaintiffs and any profits made by Trade Desk as a result of the violation or (ii) statutory damages of whichever is greater of $100 a day for each violation or $10,000.

Fourth Cause of Action
Violation of California Invasion of Privacy Act, Cal. Penal Code §§ 630 to 638 (on behalf of the Statutory Sub-Class)

242. Plaintiffs and the Statutory Sub-Class members reallege and incorporate by reference each allegation in the preceding paragraphs contained herein.

Wiretapping – California Penal Code § 631

243. The California Invasion of Privacy Act (CIPA) is codified at Cal. Penal Code §§ 630-638. The Act begins with its statement of purpose:

> The legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and

> cannot be tolerated in a free and civilized society. The Legislature by this chapter intends to protect the right of privacy of the people of this state.

Cal. Penal Code § 630 ("Legislative declaration and intent").

244. Cal. Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars.

245. Speaker of the California Assembly, Jesse Unruh, who introduced CIPA, urged that the law "represents an important advance in California law protecting the inherent rights of our citizens to privacy in their personal affairs. It is far stronger than the laws of many states in this field, and much tougher than the proposed federal eavesdropping legislation."[160] He further emphasized that the law would act as "a powerful deterrent to those who wiretap illegally for profit."[161]

246. Trade Desk is a "person" within the meaning of CIPA § 631.

247. The following items constitute "machine[s], instrument[s], or contrivance[s]" under CIPA, and even if they do not, Trade Desk's deliberate and purposeful scheme that facilitated its interceptions falls under the broad statutory catch-all category or "any other manner":

a. The computer codes and programs Trade Desk used to track Plaintiffs' and Statutory Sub-Class members' communications;

b. Plaintiffs' and Statutory Sub-Class members' browsers;

---

[160] July 31, 1967, Letter from Rep. Jesse M. Unruh to then California governor Ronald Reagan urging him to sign CIPA into law.

[161] *Id*.

c. Plaintiffs' and Statutory Sub-Class members' computing and mobile devices; and,

d. The plan Trade Desk carried out to effectuate its tracking and interception of Plaintiffs' and Statutory Sub-Class members' communications.

248. Trade Desk's source code intercepts the contents of users' communications with websites and secretly sends them to Trade Desk while the users are in the process of communicating with those websites, as described above at paragraphs 219–235.

249. Trade Desk's actions were designed to learn or attempt to learn the meaning of the contents of Plaintiffs' and Statutory Sub-Class members' communications exchanged with websites they visited.

250. Trade Desk's learning, or attempting to learn, the contents of Plaintiffs' and Statutory Sub-Class members' communications occurred while they were in transit or in the process of being sent or received. Trade Desk did not have the prior consent of all parties to learn the contents of or record the confidential communications at issue, as Plaintiffs and Statutory Sub-Class members did not provide express prior consent to Trade Desk's interception of their communications with websites

251. Trade Desk is headquartered in California, designed and effectuated its scheme to track the communications at issue here in California.

252. Plaintiffs and Statutory Sub-Class members have suffered loss by reason of these violations, including, but not limited to, violations of their rights to privacy and loss of value in their personally identifiable information.

253. Pursuant to California Penal Code § 637.2, Plaintiffs and Statutory Sub-Class members have been injured by the violations of California Penal Code § 631, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

Use of Pen Register – California Penal Code § 638.51

254. California Penal Code Section 638.50(b) defines a "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted

by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication."

255. California Penal Code Section 638.51 prohibits any person from using a pen register without a court order.

256. Courts have repeatedly recognized that in the Internet era, pen registers can take the form of software and, as a result, private companies and persons have the ability gather the same electronic information as law enforcement. The California legislature does not limit its prohibition on installing pen registers to law enforcement.

257. Trade Desk's code, as described at paragraphs 219–235 above, constitute "pen registers" because they are "devices" or "processes" that "record" "addressing or signaling information,"—such as Plaintiffs' and Statutory Sub-Class members' IP addresses—from the electronic communications transmitted by their smartphones and desktop computers. To the extent the URLs and email addresses intercepted by Trade Desk's code do not constitute contents of communications, they constitute routing, addressing, or signaling data.

258. Trade Desk's was not authorized by any court order to use a pen register to record Plaintiffs' and Statutory Sub-Class members' routing, addressing, or signaling information.

259. Trade Desk uses pen registers to collect such information *en masse* from class members as a non-party to their communications with websites, for the express purpose of creating comprehensive profiles of Plaintiffs and Statutory Sub-Class members and facilitating the tracking of all of their online activity and making that information available to third parties. The interception of data is done for the express purpose of personally identifying Plaintiffs and Statutory Sub-Class members and using that information to link Plaintiffs' and Statutory Sub-Class members' online activities to the permanent profiles Trade Desk maintains of them. The data Trade Desk collects and aggregates for use with its UID2 through its pen registers constitutes "unique fingerprinting," thereby providing unique information normally within the domain of law enforcement officers with a warrant.

260. As a direct and proximate result of Trade Desk's conduct, Plaintiffs and Statutory Sub-Class members suffered losses and were damaged in an amount to be determined at trial.

261. At all relevant times, Trade Desk's conduct alleged herein was without the authorization and consent of Plaintiffs and Statutory Sub-Class members.

262. Unless enjoined, Trade Desk will continue to commit the violations of law alleged here.

263. Plaintiffs and Statutory Sub-Class members seek all relief available under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of $5,000 per violation.

Fifth Cause of Action
Violation of the Comprehensive Computer Data Access and Fraud Act Cal. Penal Code §502 ("CDAFA") (on behalf of the Statutory Sub-Class)

264. Plaintiffs and the Statutory Sub-Class reallege and incorporate each allegation in all preceding paragraphs contained herein.

265. The California Comprehensive Computer Data Access and Fraud Act ("CDAFA") was enacted to provide protection from "tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a).

266. CDAFA affords a private right of action to owners of computers, systems, networks, programs, and who suffer damage or loss as a result of a violation of the Act. *See* Cal. Penal Code § 502(e)(1).

267. Relevant here, CDAFA imposes civil liability on anyone who:

a. Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data. Cal. Penal Code § 502(c)(1);

b. Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network. Cal. Penal Code § 502(c)(2);

c. Knowingly and without permission uses or causes to be used computer services. Cal. Penal Code § 502(c)(3);

d. Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network. Cal. Penal Code § 502(c)(4);

e. Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section. Cal. Penal Code § 502(c)(6);

f. Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network. Cal. Penal Code § 502(c)(7); and

g. Knowingly introduces any computer contaminant into any computer, computer system, or computer network. Cal. Penal Code § 502(c)(8).

268. "Computer services" under the CDAFA "includes, but is not limited to, computer time, data processing, or storage functions, internet services, electronic mail services, electronic message services, or other uses of a computer, computer system, or computer network." Cal. Penal Code § 502(b)(4).

269. "Computer network" is "any system that provides communications between one or more computer systems and input/output devices, including, but not limited to, display terminals, remote systems, mobile devices, and printers connected by telecommunication facilities." Cal. Penal Code § 502(b)(2).

270. "Computer system" is "a device or collection of devices, including support devices…one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control." Cal. Penal Code § 502(b)(5).

271. "Data" is defined as "a representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions" that "may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device." Cal. Penal Code § 502(b)(8).

272. "Computer contaminant" is defined as "any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer

system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consumer computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network." Cal. Penal Code § 502(b)(12).

273. Trade Desk's conduct, described herein, violates Cal. Penal Code §§ 502(c)(1), (2), (3), (4), (6), (7), and (8).

274. Plaintiffs and Statutory Sub-Class members were the owners or lessees of the computers, computer systems, computer networks, and data described herein.

275. In violation of Cal. Penal Code § 502(c)(8), Trade Desk knowingly introduced and continues to introduce computer contaminants into Plaintiffs' and Statutory Sub-Class members' computer, computer system, or computer network. Among other things, Trade Desk's UID2 token, Universal Pixel, Static Tracking Pixel, Real Time Conversion Events SDK, and TDID and other Trade Desk cookies are designed to, and do, self-propagate to contaminate users' computers, computer systems, and computer networks to record and transmit data that would not otherwise be transmitted or recorded in the normal operation of the computers, computer systems, and computer networks. These technologies usurp the normal operation of Plaintiffs' and Statutory Sub-Class members' computing devices because they supplant Plaintiffs' and Statutory Sub-Class members' choices in how those devices and their resources are used. For instance:

a. Trade Desk's UID2 token masquerades as a first-party identifier belonging to websites visited by Plaintiffs and Statutory Sub-Class members. When Plaintiffs and Statutory Sub-Class members provide their email addresses or phone numbers to the website, this information is hashed and stored in the UID2 token in the cookie or local storage of Plaintiffs' and Statutory Sub-Class members' computing devices as a purported "first-party" identifier. This token is then accessed and transmitted to advertisers to match the token with Plaintiffs' and Statutory Sub-Class members' internet activities in the advertising ecosystem.

b. Trade Desk's cookies, including the TDID cookie, store and cause the transmission of unique identifiers that enable Trade Desk and other entities to track Plaintiffs and Statutory Sub-Class members as they navigate websites where the cookies appear.

c. Trade Desk's pixels allow Trade Desk to intercept Plaintiffs' and Statutory Sub-Class members' information, including URLs being viewed, search queries, IP addresses, device identifiers, user-agent information, and other information and actions taken by Plaintiffs and Statutory Sub-Class members while using their devices.

d. These technologies thus cause Plaintiffs' and Statutory Sub-Class members' devices to act in ways that are contrary to that which is intended by Plaintiffs and Statutory Sub-Class members as the owners of the devices and data contained on them.

276. Trade Desk knowingly and without permission used and continues to use Plaintiffs' and Statutory Sub-Class members' data, computer, computer system, or computer network including to devise or execute its scheme or artifice to obtain money, property, or data, in violation of §§ 502(c)(1)-(3).

277. In violation of §§ 502(c)(1)-(4), (6)-(8), Trade Desk knowingly took, copied, accessed, used, caused to be used, altered, and added Plaintiffs' and Statutory Sub-Class Members' data, computers, computer services, and computer networks. Among other things, Trade Desk knowingly introduced its technologies into Plaintiffs' and Statutory Sub-Class members' computers, computer systems, and computer networks and provided itself and other entities the means of accessing Plaintiffs' and Statutory Sub-Class members' computers, computer systems, and computer networks in violation of CDAFA by developing the technologies and encouraging and providing the means for websites and other online services to use and deploy them on their platforms.

278. Trade Desk makes use of Plaintiffs' and Statutory Sub-Class members' valuable data to obtain money through advertising.

279. Trade Desk's use of Plaintiffs' and Statutory Sub-Class members' data is wrongful and unlawful, as described herein.

280. Trade Desk's use and access of Plaintiffs' and Statutory Sub-Class Members' data, computers, computer services, and computer networks, and Trade Desk's introduction of its technologies into Plaintiffs' and Statutory Sub-Class members' computers, computer services, and computer networks was without permission because:

a. Plaintiffs and Statutory Sub-Class members never authorized Trade Desk to introduce the UID2 token into their computers, computer services, or computer networks or otherwise access or use their data, computers, computer services, or computer networks via the Universal Pixel, Static Tracking Pixel, Real Time Conversion Events SDK, or TDID and other Trade Desk cookies;

b. Trade Desk's tracking technologies were invisible to Plaintiffs and Statutory Sub-Class members;

c. Plaintiffs and Statutory Sub-Class members were unaware that Trade Desk was using its tracking technologies to surreptitiously access and use Plaintiffs' and Statutory Sub-Class members' data, computers, computer services, or computer networks;

d. Trade Desk circumvented technical and/or code-based barriers to access and use Plaintiffs' and Statutory Sub-Class members' data, computers, computer services, and computer networks. For instance, Trade Desk designed the UID2 token to disguise itself as a cookie from first-party websites that Plaintiffs and Statutory Sub-Class members are visiting so that Trade Desk ensures the token is placed on the Plaintiffs' and Statutory Sub-Class members' devices. By doing so, Trade Desk circumvents the same origin policy[162] and other technical barriers.

281. None of Trade Desk's technologies are necessary for any Plaintiff's or Statutory Sub-Class member's device to communicate effectively with websites and other online services.

282. As a result of Trade Desk's violation of CDAFA, Plaintiffs and Statutory Sub-Class members have suffered damage and/or loss, including but not limited to the deprivation of control

[162] The "same origin policy" is a security mechanism in web browsers that restrict how a web page loaded from origin (i.e., domain) can interact with resources from a different origin. Among other things, the same origin policy is intended to prevent third party tracking across websites. *See*, *e.g.*, World Wide Web Consortium, *Same Origin Policy*, https://www.w3.org/Security/wiki/Same_Origin_Policy.

over their valuable property, *i.e.*, their personal information, the ability to receive compensation for their data, and the ability to withhold their data for sale.

283. Plaintiffs' and Statutory Sub-Class Members' data that Trade Desk accesses and uses is not publicly viewable and only became accessible to Trade Desk through its surreptitious and unauthorized tracking.

284. Trade Desk's violations were willful, fraudulent, and/or oppressive. Trade Desk alone created and provided its tracking technologies. Trade Desk utilized these technologies to surreptitiously intercept, collect, and compile detailed profiles of Plaintiffs' and Statutory Sub-Class member's online activity. At all times, Trade Desk was aware of how its technology functioned but made no effort to alert or obtain permission from Plaintiffs and Statutory Sub-Class members prior to deploying it on their computing devices.

285. Plaintiffs and Statutory Sub-Class Members seek actual damages, general damages, unjust enrichment, punitive damages, appropriate injunctive or other equitable relief pursuant to Cal. Penal Code § 502(e)(1) and any other relief the Court deems just. Pursuant to Cal. Penal Code § 502(e)(2), Plaintiffs and Statutory Sub-Class Members also ask the Court to award them their reasonable attorneys' fees.

286. Pursuant to Cal. Penal Code § 502(e)(4), Plaintiffs and Statutory Sub-Class Members are also entitled to punitive or exemplary damages because Trade Desk's violations are willful, and upon information and belief, Trade Desk is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

Sixth Cause of Action
Unjust Enrichment under California Common Law
(on behalf of the United States Class, or in the alternative on behalf of the California Sub-Class)

287. Plaintiffs repeat and reallege each allegation in all preceding paragraphs contained herein.

288. California common law on unjust enrichment is applicable for all members of the United States Class.

289. Trade Desk has wrongfully and unlawfully trafficked in Plaintiffs' and United States Class members' personal information and other personal information without their consent and for substantial profits.

290. Plaintiffs' and United States Class members' personal information and data have conferred an economic benefit on Trade Desk.

291. Trade Desk has been unjustly enriched at the expense of Plaintiffs and United States Class members, and the company has unjustly retained the benefits of its unlawful and wrongful conduct.

292. It would be inequitable and unjust for Trade Desk to be permitted to retain any of the unlawful proceeds resulting from its unlawful and wrongful conduct.

293. Plaintiffs and United States Class members accordingly are entitled to equitable relief including restitution and disgorgement of all revenues, earnings, and profits that Trade Desk obtained as a result of its unlawful and wrongful conduct.

294. When a defendant is unjustly enriched at the expense of a plaintiff, the plaintiff may recover the amount of the defendant's unjust enrichment even if plaintiff suffered no corresponding loss, and plaintiff is entitled to recovery upon a showing of merely a violation of legally protected rights that enriched a defendant. Trade Desk has been unjustly enriched by virtue of its violations of Plaintiffs' and United States Class members' legally protected rights to privacy as alleged herein, entitling Plaintiffs and United States Class members to restitution of Trade Desk's enrichment. "[T]he consecrated formula 'at the expense of another' can also mean 'in violation of the other's legally protected rights,' without the need to show that the claimant has suffered a loss." Restatement (Third) of Restitution § 1, cmt. a.

295. The elements for a claim of unjust enrichment are (1) receipt of a benefit and (2) unjust retention of the benefit at the expense of another. The doctrine applies where a plaintiff, while having no enforceable contract, nonetheless has conferred a benefit on defendant which defendant has knowingly accepted under circumstances that make it inequitable for the defendant to retain the benefit without paying for its value.

296. It is a longstanding principle of law embodied in the Restatement (Third) of Restitution and Unjust Enrichment (2011) that a person who is unjustly enriched at the expense of another may be liable for the amount of the unjust enrichment even if the defendant's actions caused the plaintiff no corresponding loss. Where "a benefit has been received by the defendant but the plaintiff has not suffered a corresponding loss or, in some cases, any loss, but nevertheless the enrichment of the defendant would be unjust . . . [t]he defendant may be under a duty to give to the plaintiff the amount by which [the defendant] has been enriched." Rest., Restitution, § 1, com. e.

297. The comments to the Restatement (Third) explicitly recognize that an independent claim for unjust enrichment may be predicated on a privacy tort. Restatement (Third) of Restitution and Unjust Enrichment § 44 cmt. b ("Profitable interference with other protected interests, such as the claimant's right of privacy, gives rise to a claim under § 44 if the benefit to the defendant is susceptible of measurement").

298. Because "[a] person is not permitted to profit by his own wrong," *id.* § 3, "[g]ains realized by misappropriation, or otherwise in violation of another's legally protected rights, must be given up to the person whose rights have been violated." *Id.* ch. 5, introductory note. These principles are deeply ingrained in California law. California courts have long recognized a common law claim based on unjust enrichment. In determining the remedy for such claims, California courts apply principles found in the Restatement.

299. The unauthorized use of Plaintiffs' and United States Class members' information for profit entitles them to profits unjustly earned.

300. Trade Desk has unjustly profited from tracking, disclosing, and profiting from Plaintiffs' and United States Class members' Internet activity and real-world activity to third parties without Plaintiffs' and United States Class members' knowledge or consent.

301. Plaintiffs and United States Class members did not provide authorization for the use of their personal information, nor did Trade Desk provide them with control over its use to produce revenue. This unauthorized use of their information for profit entitles Plaintiffs and United States Class members to profits unjustly earned.

302. It would be unjust and inequitable to allow Trade Desk to profit from its violation of Plaintiffs' and United States Class members' Constitutional, common law, and statutory rights as described herein.

303. Trade Desk was aware of the benefit conferred by Plaintiffs. Indeed, Trade Desk's data marketplace is premised entirely on the sale of such data to third parties. Trade Desk acted in conscious disregard of the rights of Plaintiffs and United States Class members and should be required to disgorge all profit obtained therefrom to deter Trade Desk and others from committing the same unlawful actions again.

Seventh Cause of Action
Declaratory Judgment that Trade Desk Wrongfully Accessed, Collected, Stored, Disclosed, Sold, and Otherwise Improperly Used Plaintiffs' Private Data
(on behalf of the United States Class)

304. Plaintiffs reallege and incorporate each allegation in all preceding paragraphs contained herein.

305. The gravamen of this controversy lies in Trade Desk's collection, tracking, and analysis of Plaintiffs' and United States Class members' personal information and behavior, building dossiers based on that information, and providing access to that information to third parties. Plaintiffs and United States Class members never consented to, or were even aware of, Trade Desk's conduct described herein.

306. Trade Desk's misconduct has put Plaintiffs' and United States Class members' privacy and autonomy at risk, and violated their dignitary rights, privacy, and economic well-being.

307. Accordingly, Plaintiffs seek appropriate declaratory relief, and injunctive relief as prayed for below.

X. PRAYER FOR RELIEF

308. WHEREFORE, Plaintiffs respectfully request that this Court:

a. Issue an order determining that this action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs are proper class representatives, that Plaintiffs' attorneys shall be appointed as Class counsel pursuant to Rule 23(g) of the Federal Rules of Civil Procedure, and that Class notice be promptly issued;

b. Certify this action is a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure;

c. Appoint Plaintiffs to represent the Class and Sub-Classes;

d. Appoint undersigned counsel to represent the Class and Sub-Classes;

e. Enter judgment in favor of Plaintiffs and Class members against Trade Desk awarding damages, including punitive damage, and/or nominal damages, to Plaintiffs and Class Members, in an amount according to proof at trial, including interest thereon;

f. Enter judgment in favor of Plaintiffs and Class members against Trade Desk awarding restitution of Trade Desk's ill-gotten gains, revenues, earnings, or profits that it derived, in whole or in part, from its unlawful collection and use of Class members' personal information, in an amount according to proof at trial;

A. Enter declaratory judgment in favor of Plaintiffs and Class members against Trade Desk pursuant to 28 U.S.C. § 2201 declaring that Trade Desk's conduct is unlawful as alleged herein;

B. Permanently restrain Trade Desk, and its officers, agents, servants, employees, and attorneys, from intercepting, tracking, collecting, or compiling the personal information of Class members as alleged herein;

C. Award Plaintiffs and Class members their reasonable costs and expenses incurred in this action, including attorneys' fees and expert fees; and

D. Grant Plaintiffs and Class members further equitable, injunctive, declaratory, or other relief as the Court deems appropriate.

XI. DEMAND FOR JURY TRIAL

309. Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated: July 18, 2025

Respectfully submitted,

/s/ *Michael W. Sobol*
Michael W. Sobol (SBN 194857)
msobol@lchb.com
David T. Rudolph (SBN 233457)
drudolph@lchb.com
Linnea D. Pittman (*pro hac vice*)
lpittman@lchb.com
Danna Elmasry (*pro hac vice*)
delmasry@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

/s/ *Jay Barnes*
Jason 'Jay' Barnes (*pro hac vice*)
jaybarnes@simmonsfirm.com
Eric Johnson (*pro hac vice*)
ejohnson@simmonsfirm.com
An Truong (*pro hac vice*)
atruong@simmonsfirm.com
Sona Shah (*pro hac vice*)
sshah@simmonsfirm.com
SIMMONS HANLY CONROY LLP
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel: 212-784-6400
Fax: 212-213-5949

/s/ *Christian Levis*
Christian Levis (*pro hac vice*)
clevis@lowey.com
Amanda Fiorilla (*pro hac vice*)
afiorilla@lowey.com
Rachel Kesten (*pro hac vice*)
rkesten@lowey.com
Yuanchen Lu (*pro hac vice*)
ylu@lowey.com
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035

/s/ *Philip L. Fraietta*
Philip L. Fraietta (SBN 354768)
pfraietta@bursor.com
Max S. Roberts (*pro hac vice forthcoming*)
mroberts@bursor.com

Victoria X. Zhou (*pro hac vice forthcoming*)
vzhou@bursor.com
Joshua R. Wilner (SBN 353949)
jwilner@bursor.com
BURSOR & FISHER, P.A.
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: 646.837.7150
Facsimile: 212.989.9163

Attorneys for Plaintiffs and the Proposed Classes

ATTESTATION

Pursuant to Civil Local Rule 5.1 regarding signatures, I attest that concurrence in the filing of this document has been obtained from the other signatories.

Dated: July 18, 2025

/s/ *Michael W. Sobol*

Michael W. Sobol
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP